Secure Gateway for Windows Administrator's Guide

For other guides in this document set, go to the Document Center

Secure Gateway for MetaFrame Presentation Server

Citrix® MetaFrame® Presentation Server 3.0
Citrix® MetaFrame® Access Suite

Use of the product documented in this guide is subject to your prior acceptance of the End User License Agreement. Copies of the End User License Agreement are included in the root directory of the Citrix MetaFrame product CD containing Secure Gateway for MetaFrame software.

Copyright and Trademark Notice

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of Citrix Systems, Inc.

Copyright © 2001–2004 Citrix Systems, Inc. All rights reserved.

Citrix, ICA (Independent Computing Architecture), and MetaFrame Secure Access Manager are registered trademarks, and Citrix Solutions Network, MetaFrame XP server, Program Neighborhood are trademarks of Citrix Systems, Inc. in the United States and other countries.

RSA Encryption © 1996–1997 RSA Security Inc., All Rights Reserved.

Trademark Acknowledgements

Adobe, Acrobat, and PostScript are trademarks or registered trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

ACE/Server, ACE/Agent, RSA, and SecurID are registered trademarks or trademarks of RSA Security Inc.

Microsoft, MS-DOS, Windows, Windows NT, and Win32 are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries.

All other trademarks and registered trademarks are the property of their respective owners.

Document Code: December 19, 2003 6:24 pm (SG)

Contents

Chapter 1 Before You Begin

About this Guide 9

Chapter 2 Introducing the Secure Gateway for MetaFrame Presentation Server

Overview 13
Why Use the Secure Gateway 14
What You Need 14
Securing an Access Center 14
Securing a Server Farm. 18
Secure Gateway Features 21
Where to Start. 23

Chapter 3 How the Secure Gateway Works

How the Secure Gateway Secures Your Environment 26
Connecting to an Access Center through the Secure Gateway 27
How the Secure Gateway Works 29
When Securing an Access Center. 29
When Securing a Server Farm 31
When Securing an Access Center and a Server Farm 34
When Used in a Double-hop DMZ 37
What to do Next 38

Chapter 4 Installing the Secure Gateway

Installation Prerequisites 40
For the Secure Gateway or Secure Gateway Proxy 40
For the Logon Agent 41
For the Secure Ticket Authority 41
For Client Devices 42
Web Interface Compatibility 43
MetaFrame Access Suite Components Compatibility 43

Certificate Requirements 44
In a Single-hop DMZ Deployment 45
In a Double-hop DMZ Deployment 47
Before You Install 48
Installation Sequence 48
Guidelines for Installing and Configuring Secure Gateway Components 49
Which Components You Need to Install 49
In a Single-hop DMZ Deployment 49
In a Double-hop DMZ Deployment 49
Installing the Secure Gateway 50
Configuring Secure Gateway Components 51
Upgrading Secure Gateway Components 52
Uninstalling the Secure Gateway 53
What to do Next 53

Chapter 5 Deploying the Secure Gateway with MetaFrame Secure Access Manager

Which Deployment Is Suitable For Your Organization 56
Single-hop DMZ Deployment 56
Double-hop DMZ Deployment 56
Scenario A: Single-hop DMZ Deployment 58
Printing and Completing the Pre-installation Checklist 60
Setting Up and Testing an Access Center 60
Installing the Secure Gateway and Logon Agent 61
Configuring the Logon Agent 62
Configuring the Secure Gateway 64
Checking Client Devices 65
Testing Your Deployment 65
Scenario B: Single-hop DMZ Deployment with SecurID Integration 67
Printing and Completing the Pre-installation Checklist 69
Setting Up and Testing the Access Center 69
Testing RSA SecurID Authentication on the LAN 69
Installing the Secure Gateway and Logon Agent 70
Configuring the Logon Agent 70
Configuring the Secure Gateway 73
Checking Client Devices 74
Testing Your Deployment 74

Scenario C: Double-hop DMZ Deployment 75
Printing and Completing the Pre-installation Checklist. 77
Setting Up and Testing an Access Center 77
Installing and Configuring the Logon Agent 78
Installing and Configuring the Secure Gateway Proxy 80
Installing and Configuring the Secure Gateway 82
Checking Client Devices 85
Testing Your Deployment 85

Chapter 6 Deploying Secure Gateway with Server Farms

Which Deployment Is Suitable For Your Organization 88
Single-hop DMZ Deployments 88
Double-hop DMZ Deployments. 90
Scenario A: Single-hop DMZ Deployment. 91
Printing and Completing the Pre-installation Checklist. 92
Setting Up and Testing a Server Farm 93
Installing and Configuring the STA 93
Setting Up and Testing the Web Interface 94
Installing and Configuring the Secure Gateway 95
Configuring the Web Interface to Support the Secure Gateway. 97
Checking Client Devices 97
Publishing the URL to Log On to the Secure Gateway. 97
Testing Your Deployment 97
Scenario B: Double-hop DMZ Deployment 98
Printing and Completing the Pre-installation Checklist. 100
Setting Up and Testing a Server Farm 100
Installing and Configuring the STA 100
Setting Up and Testing the Web Interface 101
Installing and Configuring the Secure Gateway Proxy 102
Installing and Configuring the Secure Gateway 104
Configuring the Web Interface to Support the Secure Gateway. 106
Publishing the URL to Log On to the Secure Gateway. 106
Checking Client Devices 106
Testing Your Deployment 107

Scenario C: Upgrading a Secure Gateway, Version 1.x Deployment 107
Printing and Completing the Pre-installation Checklist. 108
Upgrading the Server Farm 109
Upgrading and Configuring the STA 109
Upgrading and Configuring the Secure Gateway 110
Upgrading NFuse Classic 112
Locking Down IIS. 112
Publishing the URL to Log On to the Secure Gateway 113
Checking Client Devices 114
Testing Your Deployment 114

Chapter 7 Using the Secure Gateway

Tools Available When You Install the Secure Gateway 118
Using the Configuration Tools. 118
Using the Secure Gateway Management Console. 119
Viewing Secure Gateway Performance Statistics 120
Performance Counters Available for the Secure Gateway 121
Viewing Secure Ticket Authority Statistics. 124
Performance Counters Available for the STA 125
Viewing a Secure Gateway Diagnostics Report 126
Global Settings 127
Interfaces 128
Secure Gateway Proxy 128
Logon Agent 128
Authority Servers 129
Certificate Check. 129
Using the Gateway Client 130
Downloading the Gateway Client 131
How to Use the Gateway Client 132

Chapter 8 Optimization and Security Guidelines

Configuring Firewalls to Handle ICA Traffic 136

Planning for High Availability 137
Load Balancing an Array Secure Gateways 138
Load Balancing an Array of Secure Gateway Proxies 138
Certificate Requirements 138
Load Balancers and SSL Accelerator Cards 139
Using Multiple STAs 139
Keep–Alive Values and MetaFrame Presentation Server 139
Connection Keep–Alive Values and the Secure Gateway 140
Recommendations for Improving Security 142
Deploying the Secure Gateway in the DMZ 142
Restricting Ciphersuites 142
Using Secure Protocols 144
Removing Unnecessary User Accounts 144
Removing Sample Code Installed with IIS 144
Secure Components that Run on IIS 145
Stopping and Disabling Unused Services 145
Installing Service Packs and Hotfixes 145
Following Microsoft Security Guidelines 146

Chapter 9 Troubleshooting

General Troubleshooting Procedures 148
Assumptions 148
Checking Results Reported by Secure Gateway Diagnostics 148
Examining the Secure Gateway Application Log 148
Common Problems 149
Installation and Upgrade Problems 149
Certificate Problems 149
Connection Problems 150
Other Problems 152
If You Are Still Unable to Resolve the Problem 153

Appendix A About Digital Certificates 155

Understanding SSL/TLS, Cryptography, and Digital Certificates 156
SSL and TLS 156
Cryptography 156
Digital Certificates and Certificate Authorities 158

Getting Certificates 162
If Your Organization Is Its Own Certificate Authority 162
If Your Organization Is Not Its Own Certificate Authority 162
Server Certificates 163
Obtaining and Installing Server Certificates 163
Root Certificates 169
Obtaining a Root Certificate from a CA 169
Installing Root Certificates on a Client Device 169

Appendix B Error Messages 171

Checking for Error Messages 172
Secure Gateway Service Messages 173
Status Messages 173
Fatal Error Messages 174
Service Error Messages 176
Warning Messages 177
Informational Messages 180
Logon Agent Messages 181
End User Specific Messages 181
Messages Logged to the Internet Information Services (IIS) Log 181
STA Messages 183
Fatal Error Messages 183
Application Error Messages 184
Warning Messages 184
Informational Messages 185

Appendix C Glossary 187

Index 191

Before You Begin

About this Guide

This manual is designed to help anyone who plans, designs, pilots, or deploys the Secure Gateway for MetaFrame Presentation Server. It provides information to administrators about features, installation and setup, implementation, and deployment of the Secure Gateway.

The intended audience for this guide comprises experienced MetaFrame Administrators responsible for installing, configuring, and maintaining the MetaFrame Access Suite. This guide is not intended for users of the network. This guide assumes knowledge of:

- System administration
- Networking and security technologies
- Microsoft Windows 2000 Server or later
- Microsoft IIS 5.0 or later
- Internet protocols (IP, TCP, and so on)
- MetaFrame Secure Access Manager (previously known as Citrix NFuse Elite), Version 2.0
- MetaFrame Presentation Server 3.0, MetaFrame XP for Windows, Feature Release 2 or later, and MetaFrame XP for UNIX Operating Systems, Version 1.1 or later

Use this guide in conjunction with:

- *MetaFrame Secure Access Manager Administrator's Guide*
- *MetaFrame Presentation Server for Windows Administrator's Guide*
- *MetaFrame Presentation Server for UNIX Operating Systems Administrator's Guide*
- *Web Interface Administrator's Guide*

- Appropriate *Citrix MetaFrame Presentation Server Client Administrator's Guides*

The following table highlights references to typical administrative tasks and conceptual information in this guide:

Task	For more Information see …
Learn more about the MetaFrame Access Suite	The Citrix Knowledge Center at http://support.citrix.com/
Learn about digital certificates and certificate installation	"About Digital Certificates" on page 155
Install and configure the Secure Gateway	"Installing the Secure Gateway" on page 39
Using the Secure Gateway with MetaFrame Secure Access Manager	"Deploying the Secure Gateway with MetaFrame Secure Access Manager" on page 55
Using the Secure Gateway with computers running MetaFrame Presentation Server	"Deploying Secure Gateway with Server Farms" on page 87
Learn more about the Secure Gateway's performance counters and error logs	"Using the Secure Gateway" on page 117
Get general recommendations about using network components such as load balancers, SSL accelerator cards, firewalls, and so on	"Optimization and Security Guidelines" on page 135
Learn more about troubleshooting a Secure Gateway deployment	"Troubleshooting" on page 147
Get more information about error messages	"Error Messages" on page 171

Accessing Documentation

This administrator's guide is part of the MetaFrame Presentation Server documentation set. The documentation set includes online guides that correspond to different features of MetaFrame Presentation Server. Online documentation is provided as Adobe Portable Document Format (PDF) files.

Use the *Document Center* to access the complete set of online guides. The Document Center provides a single point of access to the documentation that enables you to go straight to the section of documentation that you need. The Document Center includes:

- A list of common tasks and a link to each item of documentation.
- A search function that covers all the PDF guides. This is useful when you need to consult a number of different guides.
- Cross-references among documents. You can move among documents as often as you need using the links to other guides and the links to the Document Center.

Important To view, search, and print the PDF documentation, you need to have the Adobe Acrobat Reader 5.0.5 with Search or a later version with Search. You can download Adobe Acrobat Reader for free from Adobe Systems' Web site at http://www.adobe.com/.

If you prefer to access the guides without using the Document Center, you can navigate to the component PDF files using Windows Explorer. If you prefer to use printed documentation, you can also print each guide from Acrobat Reader.

More information about Citrix documentation, and details about how to obtain further information and support, is included in *Getting Started with MetaFrame Presentation Server*, available from the Document Center.

Introducing the Secure Gateway for MetaFrame Presentation Server

Overview

The Secure Gateway for MetaFrame Presentation Server (Secure Gateway) is a MetaFrame Access Suite infrastructure component you can use to secure access to server farms and access centers. The Secure Gateway transparently encrypts and authenticates all user connections to protect against data tampering and theft.

This chapter is an overview of the capabilities and components of the Secure Gateway. It includes the following topics:

- Why Use the Secure Gateway
- What You Need
- Secure Gateway Features
- Where to Start

Why Use the Secure Gateway

Today, enterprises increasingly rely on global networks that link branch offices, telecommuters, and partners. However, the high cost of maintaining and implementing private leased lines is often prohibitive. Using cost-effective public networks—such as the Internet—is a compelling solution to this issue.

Any enterprise that relies on the Internet for connectivity must contend with security issues. Despite the enthusiasm for access at any time, any where, from any device, corporations must be certain that they can protect confidential data from prying eyes as it travels through a public network.

The Secure Gateway eases firewall traversal and provides a secure Internet gateway between MetaFrame Access Suite components and client devices.

All data traversing the Internet between a remote workstation and the Secure Gateway is encrypted using the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) security protocol. The Secure Gateway transparently encrypts and authenticates all user connections to protect against eavesdropping and data tampering.

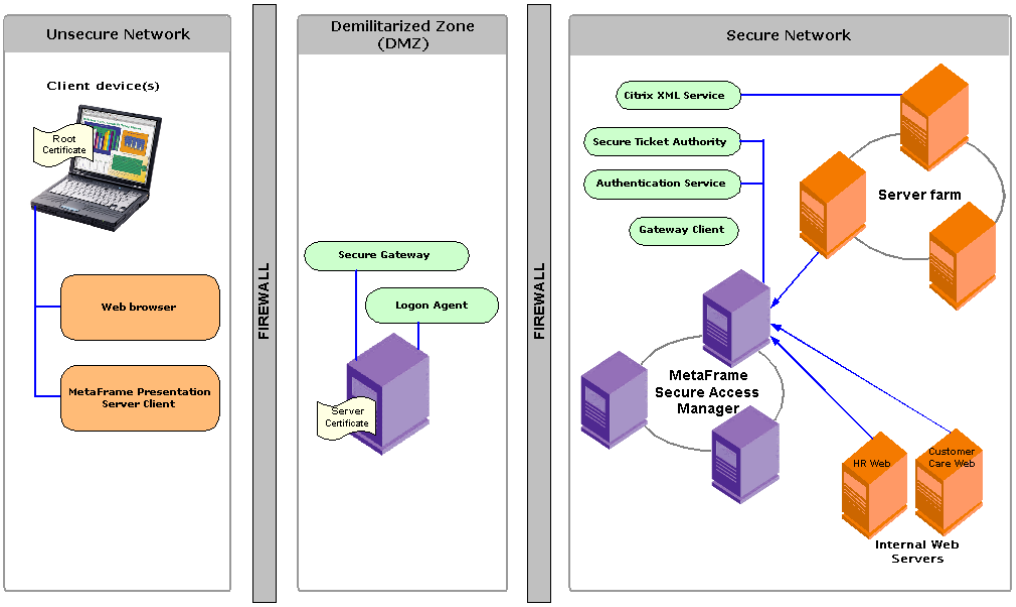
Install the Secure Gateway in a network's demilitarized zone (DMZ) to form a secure perimeter around the MetaFrame Access Suite components in your enterprise network. The Secure Gateway authenticates users connecting over the Internet and establishes a secure channel for data exchange between the client device and the MetaFrame Access Suite.

What You Need

The following sections briefly describe the components you need to install to secure access to the different components within the MetaFrame Access Suite. For detailed deployment information, see "Deploying the Secure Gateway with MetaFrame Secure Access Manager" on page 55 and "Deploying Secure Gateway with Server Farms" on page 87.

Securing an Access Center

To securely access published resources, internal data and content (from fileshares and intranets), and Internet content aggregated through an access center, you must install the Secure Gateway in the DMZ. In this configuration, the Secure Gateway manages authentication and authorization and is responsible for creating a secure channel for the native Citrix Independent Computing Architecture (ICA) and HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) traffic exchanged between the client device and servers in the secure network.



This illustration shows a typical Secure Gateway deployment used to secure an access center that aggregates content available on internal Web servers and published applications within a server farm. The unsecure network contains a client device(s) running a Web browser and MetaFrame Presentation Server Client, the demilitarized zone contains the Secure Gateway and Logon Agent components, and the secure network contains servers running MetaFrame Secure Access Manager, internal Web servers, and a server farm. MetaFrame Secure Access Manager runs the Secure Ticket Authority, Authentication Service, and Gateway Client. A server within the server farm runs the Citrix XML Service. The content from the internal Web servers and server farm is aggregated by MetaFrame Secure Access Manager. A firewall separates the unsecure network from the demilitarized zone and a second firewall separates the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate machines to enable secure communications.

In this configuration, you need the following software components:

The Secure Gateway

An application installed on a server that is typically deployed in the DMZ. The server running the Secure Gateway represents a single point of access to the access center located in a secure, enterprise network.The Secure Gateway brokers every connection request originating from the Internet to the enterprise network.

Logon Agent

The Logon Agent provides the interface that users interact with when they log on to the Secure Gateway. The Logon Agent is also responsible for facilitating the authentication of user credentials and obtaining information about the resources the user is authorized to access.

Authentication Service

A service available on a server running MetaFrame Secure Access Manager that is responsible for issuing *access tokens* in response to HTTP/S connection requests for resources available from an access center. These access tokens form the basis of authentication and authorization for HTTP/S connections to an access center.

Secure Ticket Authority (STA)

The STA is responsible for issuing *session tickets* in response to connection requests for published resources. These session tickets form the basis of authentication and authorization for access to published resources in a server farm. An instance of the STA is installed when you install MetaFrame Secure Access Manager.

Gateway Client

An ActiveX control, available on the server running MetaFrame Secure Access Manager, that downloads automatically to an authenticated, remote client browser. The Gateway Client provides the mechanism required to access internal Web servers on the enterprise network, available through the access center.

Web servers aggregated through an access center can be Web servers that host access centers, Web servers that host other Intranet Web sites (referred to as *internal Web servers*), or both. An example of an internal Web site is a Finance or Human Resources departmental Web site on the Intranet for the use of employees.

The Gateway Client is automatically downloaded and installed on the client Web browser. When installed, the Gateway Client acts as a proxy between the client browser and the Secure Gateway.

Citrix XML Service

When the Secure Gateway provides secure access to published resources available in a server farm, the Citrix XML Service is contacted for published resources availability and location.

The Citrix XML Service is the point of contact for a server farm and provides an HTTP interface to the client device. It uses TCP instead of UDP, which allows connections to work across most firewalls. The default port for the Citrix XML Service is 80. Ensure that this component is configured, functioning correctly, and is accessible through the firewall in front of the secure network.

An Access Center

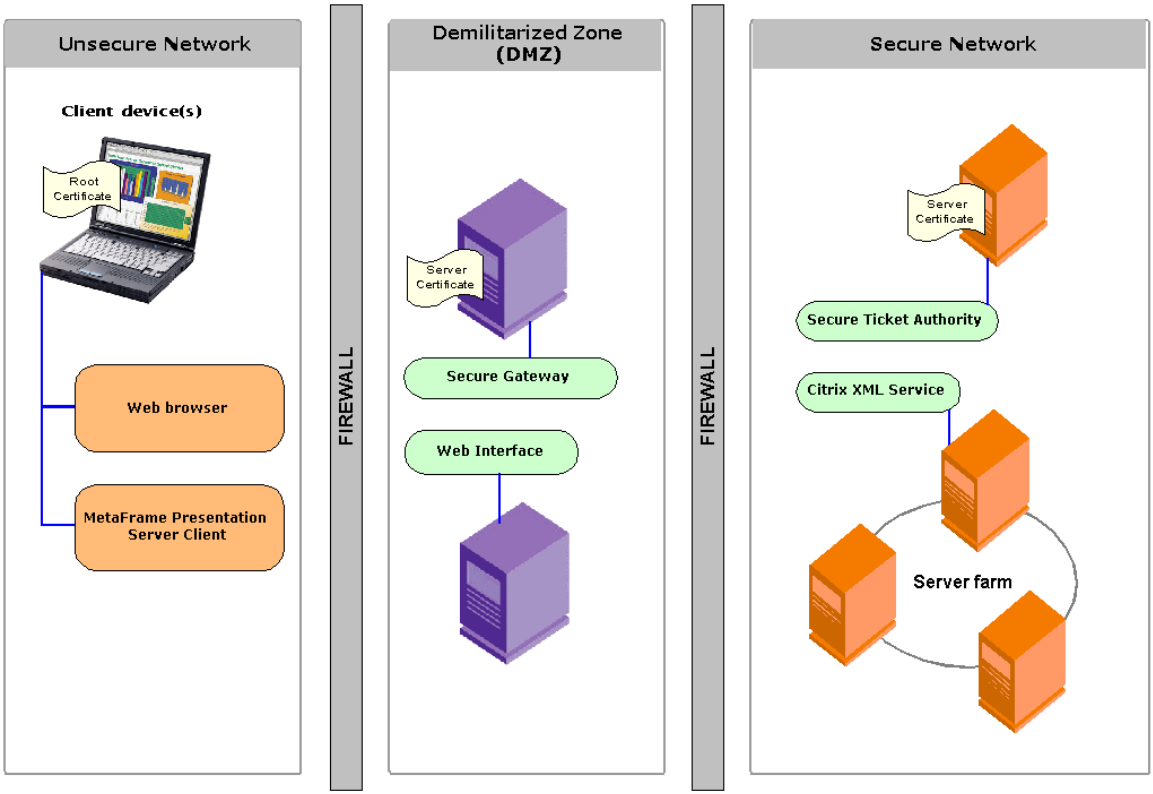
It is assumed that your enterprise network contains a server(s) running MetaFrame Secure Access Manager, and that you created an access center that allows access to Web content, internal Web servers, and published resources. For information about setting up and configuring an access center, refer to the *MetaFrame Secure Access Manager Administrator's Guide*, available from the Support area of the Citrix Web site at http://www.citrix.com/.

A Server Farm

It is assumed that your enterprise network contains one or more server farms hosting published resources that network users can access over the LAN or WAN. For information about setting up and configuring a server farm, see the *MetaFrame Presentation Server Administrator's Guide*, available from the Document Center.

Securing a Server Farm

To securely access resources published in a server farm, install the Secure Gateway in the DMZ. In this configuration, the Secure Gateway manages authentication and authorization and is responsible for creating a secure channel for data exchanged between the client device and computers running MetaFrame Presentation Server in the secure network.



This illustration shows a typical Secure Gateway deployment used to secure a server farm. The unsecure network contains a client device(s) running a Web browser and MetaFrame Presentation Server Client, the demilitarized zone contains the Secure Gateway and Web Interface components, and the secure network contains a server farm and a server running the Secure Ticket Authority. A server within the server farm runs the Citrix XML Service. A firewall separates the unsecure network from the demilitarized zone and a second firewall separates the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate machines to enable secure communications.

In this configuration, you need the following software components:

Secure Gateway

The Secure Gateway server represents a single point of access to a server farm located in a secure, enterprise network. The Secure Gateway brokers every connection request originating from the Internet to the enterprise network.

Secure Ticket Authority (STA)

The STA is responsible for issuing *session tickets* in response to connection requests for published resources. These session tickets form the basis of authentication and authorization for access to published resources in a server farm.

If you deploy the Secure Gateway for secure access to published resources in a server farm, install the STA on a stand-alone server in the secure network.

Web Interface for MetaFrame Presentation Server

When you deploy the Secure Gateway for secure Internet access to a server farm, you need to install the Web Interface in the DMZ.

The Web Interface provides user access to published resources in a server farm from a Web browser. The Web Interface works with the Secure Gateway to provide a logon interface, and facilitates authentication and authorization of connection requests to the server farm. For more information about the Web Interface, see the *Web Interface Administrator's Guide*, available from the Document Center.

Citrix XML Service

To provide secure access to published resources available in a server farm, the Secure Gateway contacts the Citrix XML Service for published resources availability and location.

The Citrix XML Service is the point of contact for a server farm and provides an HTTP interface to the client device. It uses TCP instead of UDP, which allows connections to work across most firewalls. The default port for the Citrix XML Service is 80. Ensure that this component is configured, functioning correctly, and is accessible through the firewall in front of the secure network. For more information about the Citrix XML Service, see the *MetaFrame Presentation Server Administrator's Guide*, available from the Document Center.

A Server Farm

It is assumed that your enterprise network contains a server farm with published resources that network users can access over the LAN or WAN. For information about setting up and configuring a server farm, see the *MetaFrame Presentation Server Administrator's Guides*, available from the Document Center.

Secure Gateway Features

The Secure Gateway also has the following features that were available with previous versions:

Secure Connectivity over the Internet - No VPN Required. Providing standards-based encryption over the Internet, the Secure Gateway eliminates the cost and configuration requirements of a traditional virtual private network (VPN). The Secure Gateway provides secure access to company information, corporate applications, intranets, and external Web sites without the cost and complexity of a VPN.

Supports Single-Hop or Double-Hop DMZ Deployment. The Secure Gateway can be installed to span a single-hop or a double-hop DMZ. If your DMZ is divided into two stages, install the appropriate Secure Gateway components in each DMZ segment to securely transport HTTP/S and ICA traffic to and from the secure network.

Supports Secure Communication between Secure Gateway Components. Secure Gateway components support the use of digital certificates, and the task of securing links, using SSL/TLS, between components. This is easily accomplished through user-friendly configuration wizards.

Configuration, Management, and Diagnostic Tools. The Secure Gateway Management Console, available with the Secure Gateway, is a Microsoft Management Console (MMC) snap-in you can use to manage, analyze, and troubleshoot a Secure Gateway deployment. In addition, the Secure Gateway Diagnostics tool, available from the Secure Gateway Management Console, reports configuration values, certificate details, and the state of each configured component.

Secures HTTPS Traffic. The Secure Gateway integrates seamlessly with MetaFrame Secure Access Manager to provide a secure channel for HTTPS data exchanged between client devices and the access center. If you configure access to server farms through MetaFrame Secure Access Manager, the Secure Gateway securely transports ICA as well as HTTPS traffic.

Minimal Client Configuration. When securing an access center, client devices require no preinstalled software for security. Remote, secure access is easy to support, requiring little effort from IT staff.

Secure Internet Access to Enterprise Web Servers. MetaFrame Secure Access Manager provides the ability to aggregate internal Web servers running within a LAN. When you deploy the Secure Gateway to provide secure access to an access center, remote users can access these internal Web servers as if they were connecting through the LAN. This is achieved through the Gateway Client, which is downloaded from the access center and installed as a plug-in to the user's Web browser. The Gateway Client functions as a proxy and works with the Secure Gateway to establish a secure channel to the internal Web server the user is attempting to access.

Supports RSA SecurID Integration. The Secure Gateway is designed for seamless integration with RSA SecurID authentication. If your organization invested in SecurID authentication, you can easily integrate SecurID functionality into the Secure Gateway. Users logging on through the Secure Gateway are prompted to enter valid SecurID PASSCODEs in addition to valid domain credentials.

Certificate–based security. The Secure Gateway uses standard Public Key Infrastructure (PKI) technology to provide the framework and trust infrastructure for authentication and authorization.

Standard encryption protocols. The Secure Gateway uses industry-standard SSL or TLS encryption technology to secure Web and application traffic between the client and server. It provides secure access to company information, corporate applications, intranets, and external Web sites without the cost and complexity of a VPN.

Connections between clients and the Secure Gateway are encrypted using SSL or TLS protocols. You can further enhance security by forcing the Secure Gateway to restrict its use of ciphersuites to commercial or government ciphersuites certified for Federal Information Processing Standard (FIPS) 140 requirements.

Authentication. The Secure Gateway works with the Logon Agent or the Web Interface to facilitate authentication of users attempting to establish connections to an access center. The Secure Gateway also supports two-factor authentication using RSA SecurID.

Authorization. Authorization takes place when the Secure Gateway confirms that the user is authenticated by the enterprise network. The authorization process is entirely transparent to the user.

Single point of entry. The need to publish the address of every computer running MetaFrame Presentation Server is eliminated and server certificate management is simplified. The Secure Gateway allows a single point of encryption and access to computers running MetaFrame Presentation Server.

Firewall Traversal. Connections from clients are secured with standard protocols using ports typically open on corporate firewalls. This allows easy traversal of firewalls without custom configuration.

Ease of installation and management. Adding the Secure Gateway to an existing access center is relatively quick and simple, and requires minimal configuration, significantly reducing time and management costs.

Reliability and fault tolerance. The solution allows implementation of duplicate components to enable a redundant system. Large arrays can be built using industry-standard SSL load balancing systems for scalability. Even if hardware fails, the access center remains protected.

Scalable and extensible solution. A single server running the Secure Gateway can easily support a small corporate site consisting of hundreds of users. You can support medium to large sites catering to thousands of users connecting to an array of load–balanced servers running the Secure Gateway. The Secure Gateway's components do not require any special hardware devices or network equipment upgrades.

Event and audit logging. Critical and fatal system events are logged to the Secure Gateway application log. This log file provides administrators with a record of systems events and facilitates diagnosis of system problems.

Logging levels are configurable and can be set from the user interface. Depending on the configured logging level, you can retrieve a complete record of network connection attempts to the Secure Gateway. You can also configure the Secure Gateway to omit log entries for polls from network equipment such as load balancers.

Where to Start

Review information in "How the Secure Gateway Works" on page 25 to understand how the Secure Gateway solution works and plan its deployment within your enterprise.

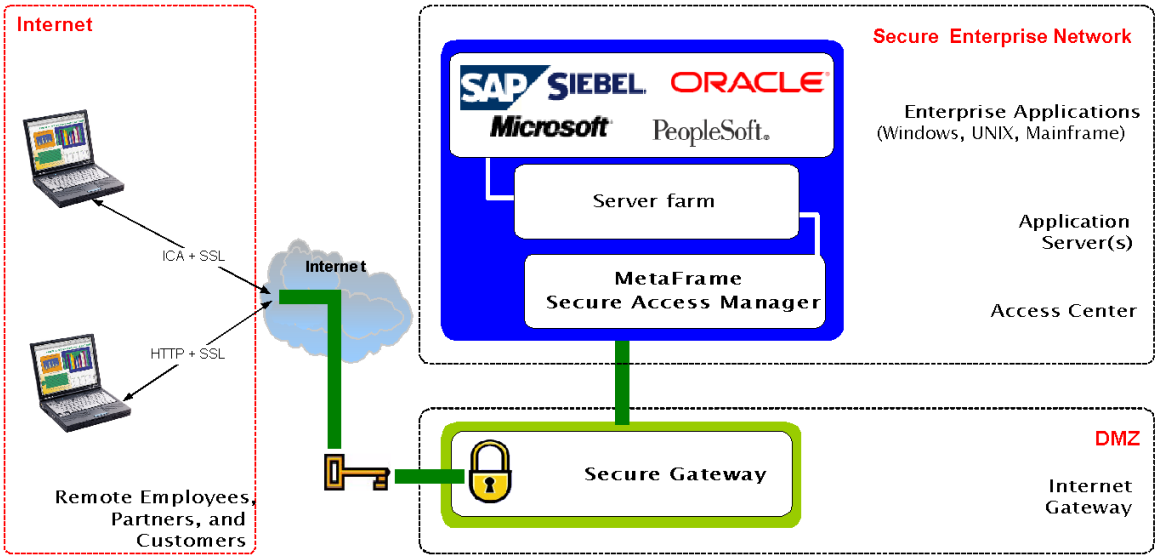
How the Secure Gateway Works

Read this chapter to understand how the Secure Gateway solution works and plan its deployment within your enterprise. This chapter contains the following topics:

- How the Secure Gateway Secures Your Environment
- How the Secure Gateway Works
- What to do Next

How the Secure Gateway Secures Your Environment

The Secure Gateway provides secure Internet access to computers running MetaFrame Presentation Server in an enterprise network.



This illustration shows how an enterprise uses the Secure Gateway to securely access information over the Internet. The network is divided into three segments. The Internet segment contains remote employees, partners, and customers. The DMZ segment contains the Secure Gateway. The Secure Enterprise Network segment contains a server farm hosting enterprise applications and MetaFrame Secure Access Manager. All data among the Internet and Secure Enterprise Network segments uses SSL and passes through the DMZ segment containing the Secure Gateway.

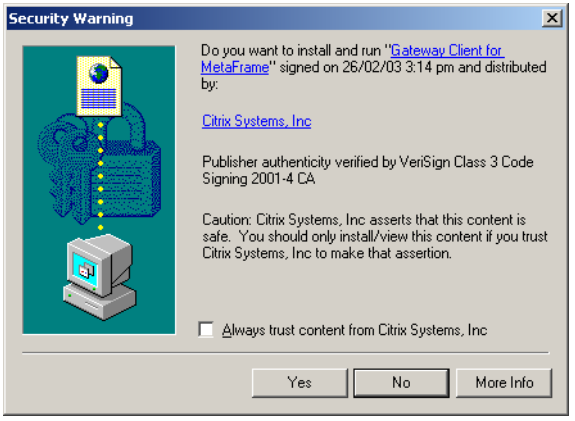
The Secure Gateway uses open standard security protocols and PKI to secure HTTP and/or ICA connections to the secure corporate network.

SSL or TLS is used to encrypt communications between remote client devices and the Secure Gateway.

Users need to log on to the secure network with valid user credentials; the Secure Gateway is completely transparent to end users. The steps required to log on to the secure network through the Secure Gateway are briefly described in the following sections.

Connecting to an Access Center through the Secure Gateway

1. Type the URL for the server running the Secure Gateway in the address bar of your Web browser. The logon screen appears.
2. Enter your user credentials for the access center and click **Login**.
3. The authentication process takes a few seconds and, if successful, a security warning prompting you to download, install, and run the Gateway Client appears.



*This illustration shows the **Security Warning** dialog box associated with the Gateway Client.*

4. Click **Yes** to proceed with download and installation of the Gateway Client. When installed, the Gateway Client provides the mechanism required to access internal Web servers aggregated through MetaFrame Secure Access Manager.

Important Citrix recommends that you ensure the Gateway Client is a genuine copy signed by Citrix Systems, Inc. before you agree to download it. Click **More Info** in the **Security Warning** dialog box for details. If in doubt about its authenticity, click **No**.

For information about using the Gateway Client, see “Using the Gateway Client” on page 130.

5. After a brief interval, the page for the access center appears.



This illustration shows a typical access center page populated with Web pages, published resources, and alert messages.

6. Click a published application icon to launch it, or browse access center content. To end your access center session, click **Log Out**.

Connecting to a Server Farm through the Secure Gateway

1. Type the URL for the server running the Secure Gateway in the address bar of your Web browser. The logon screen appears.
2. Enter your user credentials for the server farm and click **Log In**.
3. The authentication process takes a few seconds and if successful, the MetaFrame Presentation Server Applications window appears.
4. Click a published application to launch it. After a brief interval, the application you launched appears on your desktop.

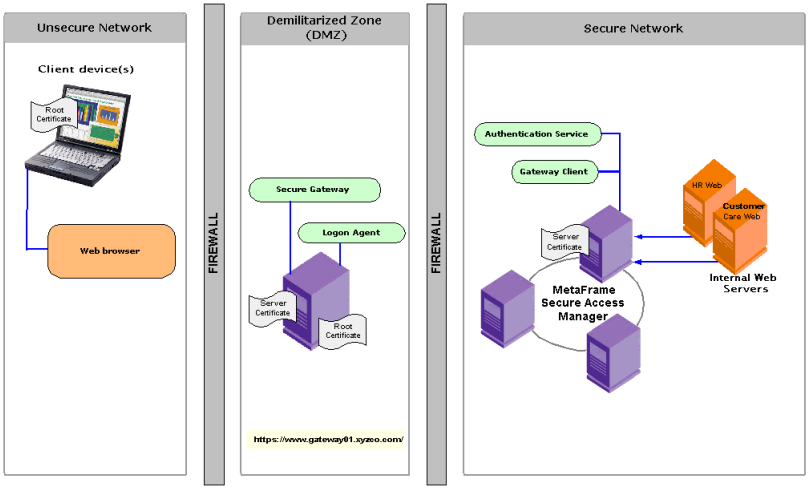
How the Secure Gateway Works

The following sections describe the interactions that take place between Secure Gateway components before a secure connection is established between a client device and the secure, enterprise network.

When Securing an Access Center

In this configuration, the Secure Gateway is deployed to provide secure access to Web content and resources available from an access center.

MetaFrame Secure Access Manager is used to aggregate Web content from one or more Web servers on the enterprise network. Mobile workers and partners are allowed to access such content over the Internet. In this usage scenario, Secure Gateway transports HTTPS traffic securely over the Internet.



This illustration shows a typical Secure Gateway deployment used to secure MetaFrame Secure Access Manager. The unsecure network contains a client device(s) running a Web browser, the demilitarized zone contains the Secure Gateway and Logon Agent components, and the secure network contains servers running MetaFrame Secure Access Manager and internal Web servers. MetaFrame Secure Access Manager runs the Authentication Service and Gateway Client. The content from the internal Web servers is aggregated by MetaFrame Secure Access Manager. A firewall separates the unsecure network from the demilitarized zone and a second firewall separates the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate machines to enable secure communications.

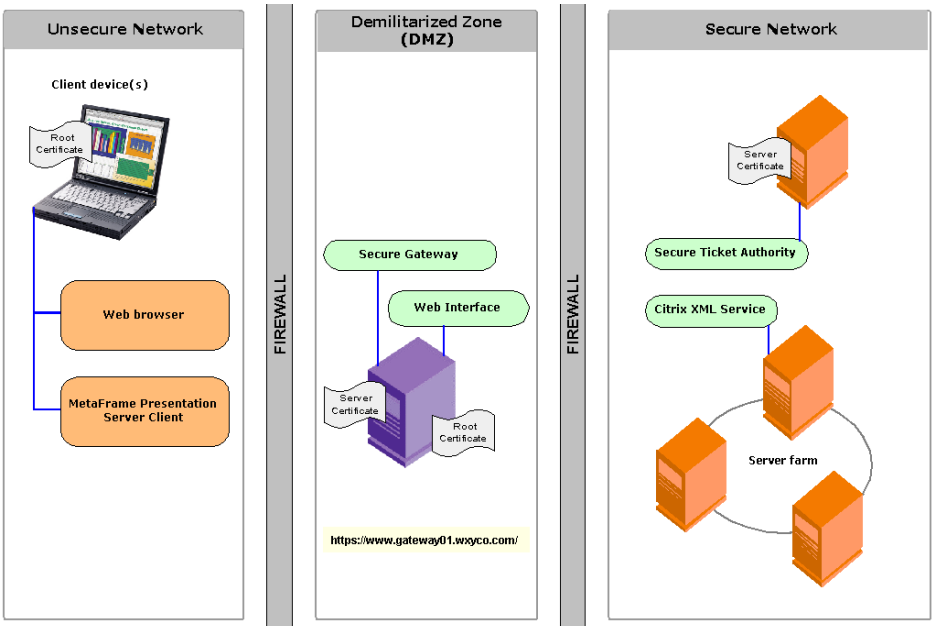
How it Works

1. A remote user types the address of the server running the Secure Gateway, for instance, https://www.gateway01.xyzco.com/, in the address field of a Web browser.
2. The Secure Gateway deployed in the DMZ receives the request and examines the contents for an access token. If no access token is present, it routes the request to the Logon Agent. If an access token is found, the Secure Gateway performs the actions described in Step 9.
3. The Logon Agent examines the URL request and sends a logon page to the Secure Gateway. The Secure Gateway sends the logon page to the client browser.
4. The user enters and submits valid logon credentials.
5. Submitted user credentials are passed to the Logon Agent through the Secure Gateway.
6. The Logon Agent forwards user credentials to the Authentication Service within the secure network.
7. The Authentication Service examines credentials, authenticates the user if credentials are valid, and generates an access token that is sent to the Logon Agent. If the credentials are invalid, a message appears on the client browser prompting the user to reenter valid user credentials.
8. The Logon Agent sends the access token to the client browser through the Secure Gateway. The access token is set on the client browser and an automatic HTTP/S request containing the embedded token is launched.
9. The Secure Gateway receives and examines the HTTP/S request. The embedded access token is found in the HTTP/S request and the Secure Gateway contacts the Authentication Service to verify the access token. The Authentication Service verifies the access token and returns the address of an access center.
10. The Secure Gateway opens a secure communications channel to the access center. When the connection is established, the Secure Gateway encrypts and decrypts data flowing through the connection.

When Securing a Server Farm

In this configuration, the Secure Gateway is deployed to provide secure Internet access directly to computers running MetaFrame Presentation Server in the enterprise.

Mobile workers and partners are allowed to access enterprise applications and resources, such as network printers, published on a server farm. In this usage scenario, the Secure Gateway securely transmits ICA traffic over the Internet.



This illustration shows a typical Secure Gateway deployment used to secure a server farm. The unsecure network contains a client device(s) running a Web browser and MetaFrame Presentation Server Client, the demilitarized zone contains the Secure Gateway and Web Interface components installed on the same server, and the secure network contains a server farm and a server running the Secure Ticket Authority. A server within the server farm runs the Citrix XML Service. A firewall separates the unsecure network from the demilitarized zone and a second firewall separates the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate machines to enable secure communications.

How it Works

In this scenario, the Secure Gateway works in conjunction with the Web Interface to provide secure access to published resources available on a secure enterprise network.

1. A remote user types the address of the server running the Secure Gateway, for instance, https://www.gateway01.wxyco.com/, in the address field of a Web browser.
2. The Secure Gateway deployed in the DMZ receives the request and relays the request to the Web Interface.
3. The Web Interface responds by sending a logon page to the client browser.
4. The user enters and submits valid user credentials that are routed to the Web Interface through the Secure Gateway.
5. The Web Interface sends user credentials to the Citrix XML Service available from the server farm in the secure network, and obtains a list of applications that this user is authorized to access.
6. The Web Interface populates the Web page with the list of published resources that the user is authorized to access.
7. When the user clicks a published application link, the Web Interface sends the IP address and port for the requested computer running MetaFrame Presentation Server to the STA and requests a session ticket for the user. The STA saves the IP address and issues the requested ticket to the Web Interface.
8. The Web Interface generates an ICA file containing the ticket issued by the STA and sends it to the client browser.

Important The ICA file generated by the Web Interface contains the FQDN or DNS name of the server running the Secure Gateway. The address of the server(s) running MetaFrame Presentation Server is never revealed to the MetaFrame Presentation Server Client.

---

9. The client Web browser uses the ICA file to launch the MetaFrame Presentation Server Client. The Client connects to the Secure Gateway using the FQDN or DNS name in the ICA file. Initial SSL/TLS handshaking is performed to establish the identity of the server running the Secure Gateway.
10. The Secure Gateway receives the session ticket from the Client and contacts the STA for ticket validation.

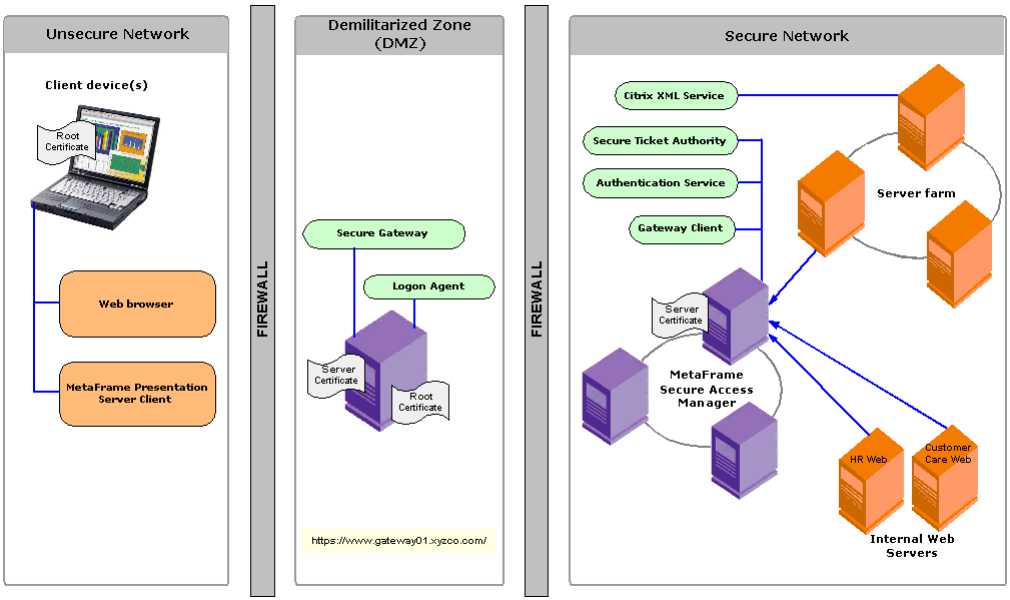
    If the ticket is valid, the STA returns the IP address of the computer running MetaFrame Presentation Server on which the requested application resides. If the session ticket is invalid or has expired, the STA informs the Secure Gateway and an error message appears on the client device.
11. On receipt of the IP address for the computer running MetaFrame Presentation Server, the Secure Gateway establishes an ICA connection to the computer. When the ICA connection is established, the Secure Gateway encrypts and decrypts data flowing through the connection.

In this deployment scenario, the Web Interface is installed on the same server as the Secure Gateway. This is a supported configuration; however, you may prefer to install the Web Interface on a separate Web server depending on the hardware resources you have available. See “Deploying Secure Gateway with Server Farms” on page 87 for detailed instructions about deploying the Secure Gateway in this scenario.

When Securing an Access Center and a Server Farm

In this configuration, the Secure Gateway provides secure Internet access to enterprise resources aggregated through MetaFrame Secure Access Manager, including published resources hosted on computers running MetaFrame Presentation Server.

Mobile workers and partners are allowed to access both Web content and published resources over the Internet. In this usage scenario, the Secure Gateway transmits HTTP and ICA traffic securely over the Internet.



This illustration shows a typical Secure Gateway deployment used to secure an access center that aggregates content available on internal Web servers and published applications within a server farm. The unsecure network contains a client device(s) running a Web browser and MetaFrame Presentation Server Client, the demilitarized zone contains the Secure Gateway and Logon Agent components, and the secure network contains servers running MetaFrame Secure Access Manager, internal Web servers, and a server farm. MetaFrame Secure Access Manager runs the Secure Ticket Authority, Authentication Service, and Gateway Client. A server within the server farm runs the Citrix XML Service. A firewall separates the unsecure network from the demilitarized zone and a second firewall separates the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate machines to enable secure communications.

How it Works

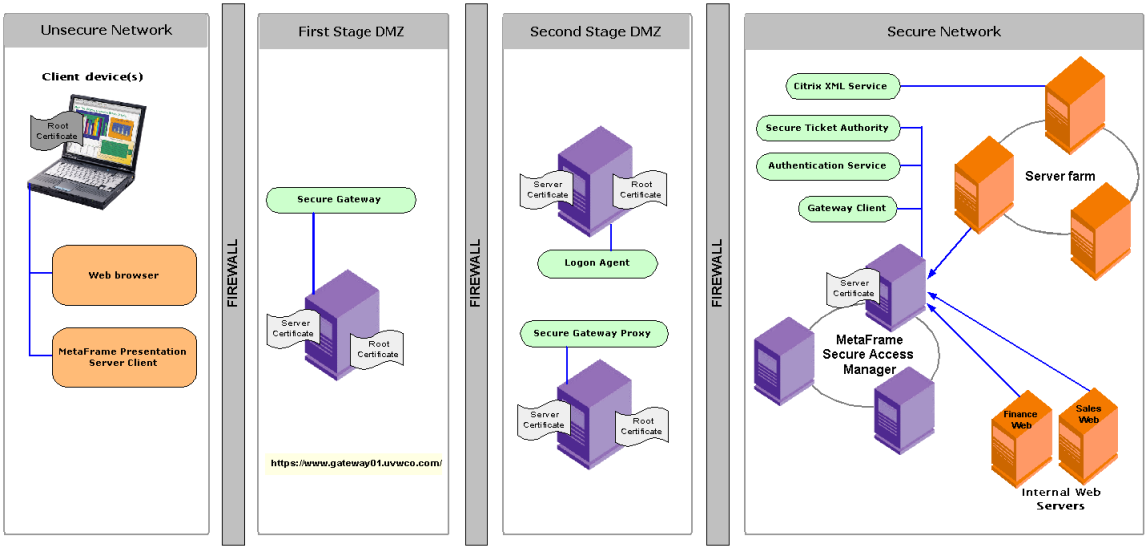
1. A remote user types the address of the server running the Secure Gateway, for instance, https://www.gateway01.xyzco.com/, in the address field of a Web browser.
2. The Secure Gateway deployed in the DMZ examines the connection request for an "access token." If no access token is present, it routes the request to the Logon Agent. If an access token is found, the Secure Gateway performs the actions described in Step 7.
3. The Logon Agent examines the connection request and sends the logon page to the Secure Gateway. The Secure Gateway sends the logon page to the client browser.
4. The user enters and submits logon credentials. Submitted user credentials are passed to the Logon Agent through the Secure Gateway. The Logon Agent forwards user credentials to the Authentication Service deployed in the secure network.
5. The Authentication Service examines credentials, authenticates the user if credentials are valid, and generates an access token that is sent to the Logon Agent. If the credentials are invalid, a message appears on the client browser prompting the user to reenter valid logon credentials.
6. The Logon Agent sends the access token to the client browser through the Secure Gateway. The access token is set on the client browser and an automatic HTTP/S request containing the embedded access token is launched.
7. The Secure Gateway receives and examines the HTTP/S request. The embedded access token is found in the HTTP/S request and the Secure Gateway contacts the Authentication Service to verify the access token. The Authentication Service verifies the access token and returns the address of an access center.
8. The Secure Gateway opens a secure communications channel to the access center. The access center page is displayed on the client Web browser. The user can access Web or application resources available through the access center.
9. To access a published resource on a computer running MetaFrame Presentation Server, the user clicks the icon for a published resource on the access center page.
10. The access center contacts the Citrix XML Service on the server farm for the application requested by the user. The Citrix XML Service returns a server address.

11. The access center sends the address for the requested computer running MetaFrame Presentation Server to the STA and requests a session ticket for the user. The STA saves the server address and returns a session ticket to the access center.
12. The access center generates an ICA file containing the session ticket issued by the STA and sends it to the client browser.
13. The Web browser uses the ICA file to launch the Client. The Client connects to the Secure Gateway using the FQDN or DNS name in the ICA file. Initial SSL/TLS handshaking is performed to establish the identity of the server running the Secure Gateway.
14. The Secure Gateway examines the session ticket from the Client and uses information contained in the ticket to identify and contact the STA for ticket validation. If the ticket is valid, the STA returns the address of the computer running MetaFrame Presentation Server on which the requested application resides. If the ticket is invalid or has expired, the STA informs the Secure Gateway and an error message appears on the client device.
15. On receipt of the IP address for the computer running MetaFrame Presentation Server, the Secure Gateway opens an ICA connection to the computer. When the ICA connection is established, the Secure Gateway encrypts and decrypts data flowing through the connection.

When Used in a Double-hop DMZ

Depending on the security and network policies practiced by your organization, the network may contain a DMZ that's divided into two stages, referred to as a *double-hop DMZ*.

The Secure Gateway is designed to fully support deployment in a double-hop scenario. To deploy the Secure Gateway in a double-hop DMZ, install the Secure Gateway in the first DMZ segment and the Logon Agent and the Secure Gateway Proxy on separate servers in the second DMZ segment. The Secure Gateway Proxy functions 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.



This illustration shows a typical double-hop Secure Gateway deployment used to secure an access center that aggregates content available on internal Web servers and published applications within a server farm. The unsecure network contains a client device(s) running a Web browser and MetaFrame Presentation Server Client, the first stage of the demilitarized zone contains the Secure Gateway, the second stage of the DMZ contains the Secure Gateway Proxy and Logon Agent components, and the secure network contains servers running MetaFrame Secure Access Manager, internal Web servers, and a server farm. MetaFrame Secure Access Manager runs the Secure Ticket Authority, Authentication Service, and Gateway Client. A server within the server farm runs the Citrix XML Service. The content from the internal Web servers and server farm is aggregated by MetaFrame Secure Access Manager. A firewall separates the unsecure network from the first stage of the demilitarized zone, a second firewall separates the first stage of the demilitarized zone from the second stage of the demilitarized zone, and the a third firewall separates the second stage of the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate machines to enable secure communications.

How it Works

The illustration above shows a double-hop deployment in which the Secure Gateway provides secure access to an access center and a server farm.

All communications between the Secure Gateway and servers within the secure network are routed through the Secure Gateway Proxy. The Secure Gateway Proxy uses an inbound access control list (ACL) to accept incoming connections from the Secure Gateway. It uses an outbound ACL to connect to specific servers within the secure network.

The communications flow is similar to those described in single-hop deployment scenarios except that any data exchanged between the Secure Gateway and servers within the secure network is proxied through the Secure Gateway Proxy.

In double-hop DMZ deployments, the server running the Logon Agent or the Web Interface must be located in the second DMZ segment.

Important If the communications link between the Secure Gateway and the Secure Gateway Proxy is not secured, port 1080 must be open on the firewall between the first DMZ segment and the second.

For more information about double-hop deployment scenarios, see "Deploying the Secure Gateway with MetaFrame Secure Access Manager" on page 55 and "Deploying Secure Gateway with Server Farms" on page 87.

What to do Next

Read "Installing the Secure Gateway" on page 39 for information about hardware, software, certificate requirements, and information about installing the Secure Gateway.

Installing the Secure Gateway

This chapter lists system requirements and provides instructions for installing and configuring the Secure Gateway. This chapter contains the following topics:

- Installation Prerequisites
- Certificate Requirements
- Before You Install
- Which Components You Need to Install
- Installing the Secure Gateway

Installation Prerequisites

Before proceeding further, ensure that the servers on which you intend to install Secure Gateway components meet the minimum hardware and software requirements described below.

For the Secure Gateway or Secure Gateway Proxy

Review the following requirements to ensure that the server on which you intend to install the Secure Gateway or Secure Gateway Proxy meets the installation prerequisites:

Server Hardware	Server Software
Recommended minimum requirements for Microsoft Windows 2000 Server Family or later. Refer to the product documentation or see the Microsoft Web site for more information.	Microsoft Windows 2000 Server Family or later with the latest service pack available.
512 MB of RAM.	
Additional 150 MB of available hard disk space.	
Network Interface Card (NIC).	

Important For maximum security, Citrix recommends you reserve this server for the Secure Gateway.

For the Logon Agent

Review the following minimum requirements to ensure that the server on which you intend to install the Logon Agent meets installation prerequisites:

Server Hardware	Server Software
Recommended minimum requirements for Microsoft Windows 2000 Server Family or later. Refer to the product documentation or see the Microsoft Web site for more information.	Microsoft Windows 2000 Server Family or later with the latest service pack available.
Additional 150 MB of available hard disk space.	Internet Information Services (IIS) 5.0, installed by default on Windows 2000 Servers.
Network Interface Card (NIC).	**Optional**. RSA ACE/Agent. This component must be installed if you want to install the Logon Agent with support for RSA SecurID authentication.

For the Secure Ticket Authority

Review the following requirements to ensure that the server on which you intend to install the STA meets installation prerequisites.

Server Hardware	Server Software
Recommended minimum requirements for Microsoft Windows 2000 Server Family or later. Refer to the product documentation or see the Microsoft Web site for more information.	Microsoft Windows 2000 Server Family or later with the latest service pack available.
256 MB of RAM.	Internet Information Services (IIS) 5.0 or later.
Additional 150 MB of available hard disk space.	
Network Interface Card (NIC).	

For Client Devices

The client device requirements depend on whether your users connect to an access center or directly to a server farm.

If Your Users Are Connecting to an Access Center

For users connecting to an access center through the Secure Gateway, client devices must meet or exceed the following requirements:

Hardware	Software
Standard PC architecture, required to run Internet Explorer 5.0 or later.	Compatible 32-bit Windows operating systems
Pointing device	Internet Explorer, Version 5.0, 5.5, or 6.0 If you are running Internet Explorer Version 5.0, ensure Microsoft Internet Explorer High Encryption Pack is installed. Citrix recommends installing the latest Service Pack. See the Microsoft Web site for more information.
Network Interface Card (NIC)	Trusted root certificates required to connect to the server running the Secure Gateway.
	Network/Internet connectivity

Important To install and run the Gateway Client required for access to internal Web servers aggregated through MetaFrame Secure Access Manager, client devices must be running a 32-bit Windows operating system and running Internet Explorer 5.0 or later.

If Your Users Are Connecting to a Server Farm

To access resources published on a server farm through the Secure Gateway, client devices must meet or exceed the following requirements:

Hardware	Software
Standard PC architecture, required to run the MetaFrame Presentation Server Client, Version 6.30 or later. See the appropriate *MetaFrame Presentation Server Client Administrator's Guide* for more information.	Compatible operating system
Pointing device	A Web browser (as required to connect to a server running the Web Interface). See the Web Interface Administrator's Guide, available from the Document Center, for a list of supported Web browsers. If you are running Internet Explorer Version 5.0, ensure Microsoft Internet Explorer High Encryption Pack is installed. Citrix recommends installing the latest Service Pack. See the Microsoft Web site for more information.
Network Interface Card (NIC)	MetaFrame Presentation Server Client (Version 6.30 or later) software
	Trusted root certificates required to connect to the server running the Secure Gateway.
	Network/Internet connectivity

Web Interface Compatibility

Secure Gateway, Version 2.0, is compatible with the Web Interface for MetaFrame Presentation Server, Web Interface for MetaFrame XP, and NFuse Classic, Version 1.7.

MetaFrame Access Suite Components Compatibility

Secure Gateway, Version 2.0, is compatible with the following MetaFrame Access Suite products:

- MetaFrame Presentation Server 3.0
- MetaFrame XP Server for Windows with Feature Release 2 or later
- MetaFrame Secure Access Manager, Version 2.0
- MetaFrame Server for UNIX Operating Systems, Version 1.1 or later

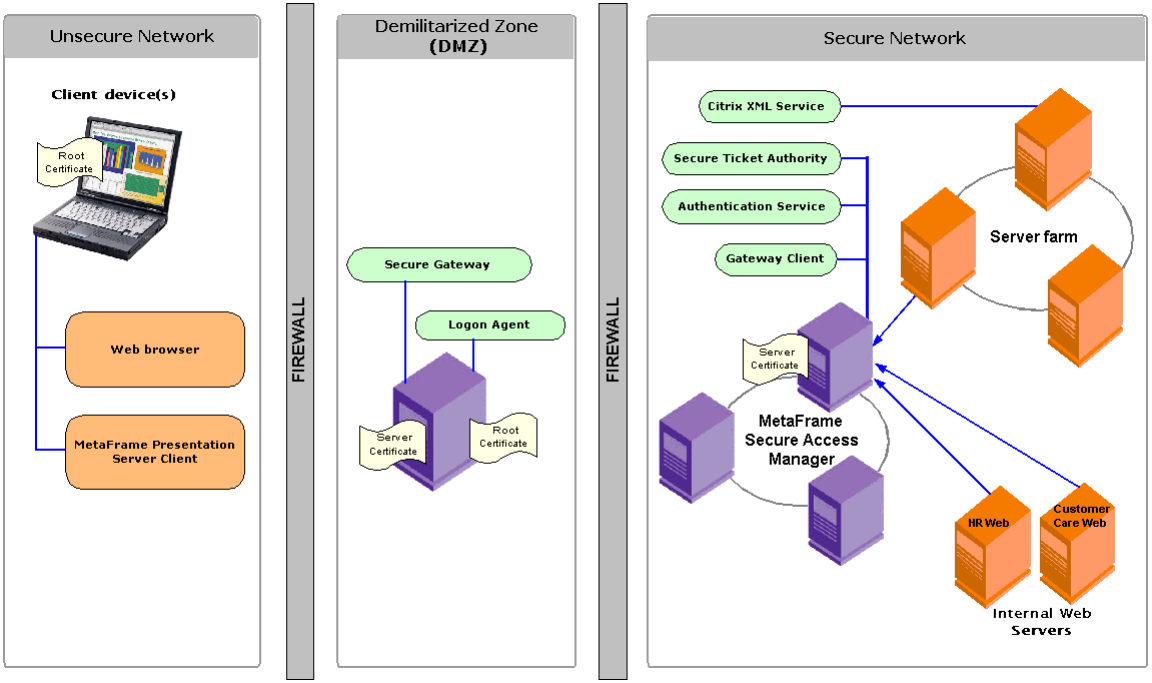
Certificate Requirements

All client devices and secure servers in a Secure Gateway deployment use digital certificates to verify each other's identity and authenticity.

For conceptual information about digital certificates and cryptography, see "About Digital Certificates" on page 155.

Important If you purchased server certificates from a commercial certificate authority (CA), support for root certificates for most commercial CAs is built into Internet Explorer and Windows server products. If you obtained server certificates from a private CA or commercial CA whose root certificates are not, by default, supported by the Windows operating system, you must install matching root certificates on all client devices and servers connecting to secure servers.

In a Single-hop DMZ Deployment



This illustration shows a typical Secure Gateway deployment used to secure an access center that aggregates content available on internal Web servers and published applications within a server farm. The unsecure network contains a client device(s) running a Web browser and MetaFrame Presentation Server Client, the demilitarized zone contains the Secure Gateway and Logon Agent components, and the secure network contains servers running MetaFrame Secure Access Manager, internal Web servers, and a server farm. MetaFrame Secure Access Manager runs the Secure Ticket Authority, Authentication Service, and Gateway Client. A server within the server farm runs the Citrix XML Service. The content from the internal Web servers and server farm is aggregated by MetaFrame Secure Access Manager. A firewall separates the unsecure network from the demilitarized zone and a second firewall separates the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate machines to enable secure communications.

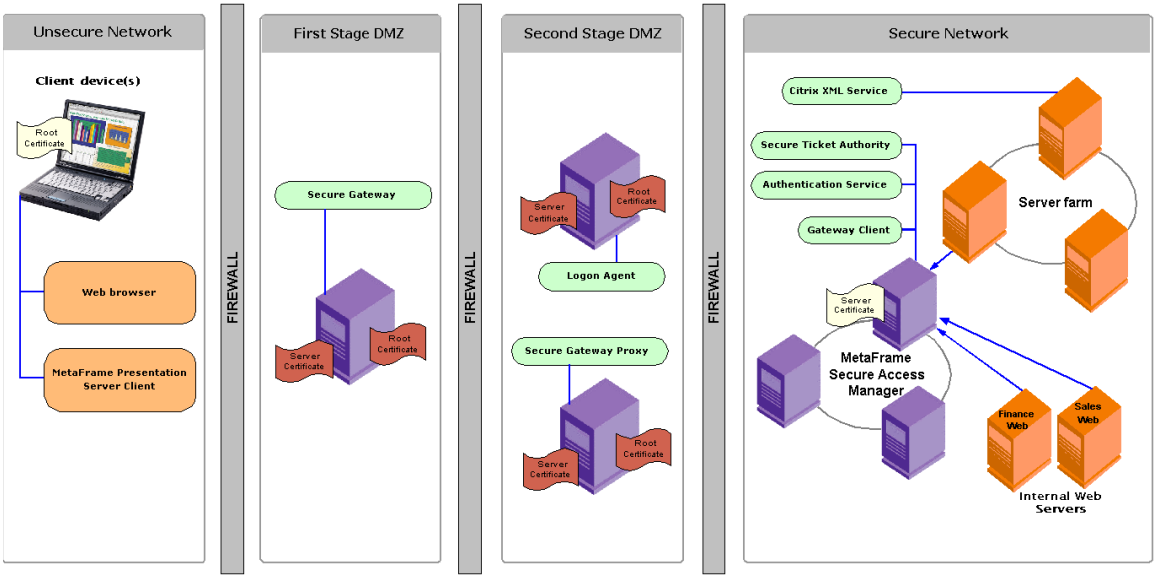
Per the illustration shown on page 44, if your network contains a single-hop DMZ, you need these certificates.

- Root certificates on all client devices that connect to the server running the Secure Gateway.

- Root certificates on every Secure Gateway component that connects to a secure server. For example, in the previous illustration, a root certificate must be present on the server running the Secure Gateway to verify the server certificate installed on the server running the Authentication Service or the STA.
- A server certificate on the server running the Secure Gateway.
- **Optional**. A server certificate on the server running the Logon Agent—required only when the Logon Agent is installed on a separate server, and you require secure communications between the Secure Gateway and the Logon Agent.
- **Optional**. A server certificate on the server running the STA and the Authentication Service. The STA and the Authentication Service are installed by default when you install MetaFrame Secure Access Manager.

All Secure Gateway components support the use of digital certificates. You, as the security administrator, need to decide whether or not the communication links between the Secure Gateway and other servers in the DMZ or secure network need to be encrypted.

In a Double-hop DMZ Deployment



This illustration shows a typical double-hop Secure Gateway deployment used to secure an access center that aggregates content available on internal Web servers and published applications within a server farm. The unsecure network contains a client device(s) running a Web browser and MetaFrame Presentation Server Client, the first stage of the demilitarized zone contains the Secure Gateway, the second stage of the DMZ contains the Secure Gateway Proxy and Logon Agent components, and the secure network contains servers running MetaFrame Secure Access Manager, internal Web servers, and a server farm. MetaFrame Secure Access Manager runs the Secure Ticket Authority, Authentication Service, and Gateway Client. A server within the server farm runs the Citrix XML Service. The content from the internal Web servers and server farm is aggregated by MetaFrame Secure Access Manager. A firewall separates the unsecure network from the first stage of the demilitarized zone, a second firewall separates the first stage of the demilitarized zone from the second stage of the demilitarized zone, and the a third firewall separates the second stage of the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate machines to enable secure communications.

Per the illustration above, if your network contains a double-hop DMZ, you need these certificates:

- Root certificates on all client devices connecting to the server running the Secure Gateway.

- Root certificates on every Secure Gateway component that connects to a secure server or Web server. For example, in the illustration above, an appropriate root certificate must be present on the server running the Secure Gateway to verify the server certificate installed on the server running MetaFrame Secure Access Manager.
- A server certificate on the server running the Secure Gateway.
- **Optional**. A server certificate on the server(s) running the Secure Gateway Proxy.
- **Optional**. A server certificate on the server running the Logon Agent.
- **Optional**. A server certificate on the server running the STA and the Authentication Service.

All Secure Gateway components support the use of digital certificates. You, as the security administrator, need to decide whether or not the communication links between the Secure Gateway and other servers in the DMZ or secure network need to be encrypted.

Before You Install

- Ensure your hardware and software meet installation prerequisites as described in "Installation Prerequisites" on page 40.
- Install certificates on servers; see "Certificate Requirements" on page 44.
- Print and complete tasks and information described in the *Secure Gateway Pre-installation Checklist*, available from the Documentation Center. Keep the completed checklist nearby when you install the Secure Gateway.

Installation Sequence

The Secure Gateway is designed to discover and verify the existence of the other Secure Gateway components during configuration. For example, when you configure the Secure Gateway, it verifies that servers running the Logon Agent, the Web Interface, the STA, and the Authentication Service, if used, are functional. If a required component is not found, the Secure Gateway may fail to start. It is therefore important to follow the recommended installation sequence.

1. Always install components within the secure network first.
2. **Optional**. If your network contains a double-hop DMZ, install components in the second DMZ segment next.
3. Install components in the first DMZ segment last.

Guidelines for Installing and Configuring Secure Gateway Components

To ensure that the security of a Secure Gateway component is not compromised, Citrix recommends:

- Reserving servers for the exclusive use of Secure Gateway components
- Ensuring only users with administrative privileges are allowed to install Secure Gateway components
- When the installation is complete, modifying access privileges to Secure Gateway executables to ensure that only users with administrative privileges have execute rights

Which Components You Need to Install

The tables below describe the components required in single and double-hop DMZ deployment scenarios.

In a Single-hop DMZ Deployment

To provide secure access to...	In the DMZ, install...	In the secure network, install...
An access center (HTTP and ICA data)	• Secure Gateway • Logon Agent	• MetaFrame Secure Access Manager • MetaFrame Presentation Server
A server farm (ICA data only)	• Secure Gateway • Web Interface	• STA • MetaFrame Presentation Server

In a Double-hop DMZ Deployment

To provide secure access to...	In the first DMZ segment, install...	In the second DMZ segment, install...	In the secure network, install...
An access center (HTTP and ICA data)	Secure Gateway	• Secure Gateway Proxy • Logon Agent	• MetaFrame Secure Access Manager • MetaFrame Presentation Server
A server farm (ICA data only)	Secure Gateway	• Secure Gateway Proxy • Web Interface	• STA • MetaFrame Presentation Server

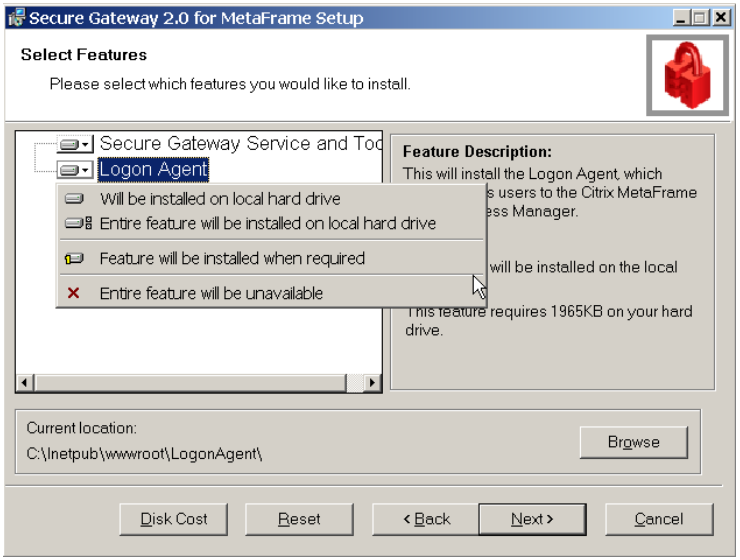
Installing the Secure Gateway

The Secure Gateway installer is designed so you can install the Secure Gateway and the Logon Agent, or the Secure Gateway Proxy. To install a Secure Gateway component, do the following:

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Gateway**. The installation wizard is launched and after a brief interval during which the installer checks the server for installed applications, the **Select Components** dialog box appears.
4. In the **Installation Mode** section, select one of the following options:
   - **Secure Gateway Service**: Select this option to install the Secure Gateway software. If you choose to install the Secure Gateway, you are also given the option of installing the Logon Agent. The Logon Agent can be installed in **Basic** mode or with support for **RSA SecurID integration**.
   - **Secure Gateway Proxy**: Select this option if your network contains a double-hop DMZ and you want to install the Secure Gateway Proxy in the second DMZ segment.
5. In the **Citrix MetaFrame products to secure** section, select the types of MetaFrame Access Suite servers the Secure Gateway will secure:
   - **MetaFrame Secure Access Manager and MetaFrame XP Server**: Select this option to deploy the Secure Gateway to provide secure Internet access to servers running MetaFrame Secure Access Manager (HTTPS data) and MetaFrame Presentation Server (ICA data).
   - **MetaFrame Secure Access Manager**: Select this option to provide secure Internet access to servers running MetaFrame Secure Access Manager (HTTPS data only).
   - **MetaFrame XP Server**: Select this option to provide secure Internet access directly to resources published on computers running MetaFrame Presentation Server (ICA data only).

   Click **Next**.
6. Read and accept the license agreement and click **Next**.
7. View information specific to the installation of the software and click **Next**.

8. In the **Select Features** dialog box, click the component you want to install and select **Will be installed on local hard drive** from the menu displayed. If you want to install a component on a different server, select **Entire feature will be unavailable**.



*This illustration shows the **Select Features** configuration options when installing the Secure Gateway.*

9. Click **Next**.

10. Click **Finish** in the **Ready to Install the Application** dialog box. The installation program starts.

Important If you cancel the installation at any point, the selections you made in the installation wizard are not saved.

Configuring Secure Gateway Components

Configuration wizards for each Secure Gateway component are launched when the installation is complete. Each configuration wizard guides you through configuration tasks and provides context-sensitive help describing the procedures and information you need to enter.

Deployment-specific configuration instructions for each Secure Gateway component are described in “Deploying the Secure Gateway with MetaFrame Secure Access Manager” on page 55 and “Deploying Secure Gateway with Server Farms” on page 87.

Upgrading Secure Gateway Components

You can upgrade previous versions of the Secure Gateway or the STA to Version 2.0.

When you run the Secure Gateway installer, it automatically checks for installed versions of the Secure Gateway. If a previously installed version of the Secure Gateway is detected, you are prompted to upgrade or remove the previous version.

Important The Secure Gateway does support upgrading the Secure Gateway when installed in relay mode. Use **Add/Remove Programs** to uninstall the software before running the Secure Gateway installer.

Upgrades are not available for the Secure Gateway Proxy and the Logon Agent. These components are new to the Secure Gateway, Version 2.0.

Uninstalling the Secure Gateway

You can uninstall the Secure Gateway using Add/Remove Programs available from the Control Panel.

To uninstall the Secure Gateway

1. Exit any applications running on the server.
2. Choose **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.
3. Select **Secure Gateway 2.0 for MetaFrame**, and click **Remove**.

If you installed the Secure Gateway and the Logon Agent on a single server and want to uninstall one of the components, see the instructions in "To uninstall a Secure Gateway component" on page 53.

To uninstall a Secure Gateway component

1. Exit any applications running on the server.
2. Choose **Start** > **Settings** > **Control Panel** > **Add/Remove Programs**.
3. Select **Secure Gateway 2.0 for MetaFrame**, and click **Change**.
4. Click **Modify** in the **Installation Maintenance** dialog box. Click **Next**.
5. In the **Select Features** dialog box, click the component you want to remove and select **Entire Feature will be unavailable**. Click **Next**. The component you selected is removed from the server.

What to do Next

For information about recommended deployment scenarios and step-by-step instructions for installing and configuring the Secure Gateway, see "Deploying the Secure Gateway with MetaFrame Secure Access Manager" on page 55 or "Deploying Secure Gateway with Server Farms" on page 87.

Deploying the Secure Gateway with MetaFrame Secure Access Manager

This chapter describes recommended scenarios for deploying the Secure Gateway to provide secure Internet access to an access center server running MetaFrame Secure Access Manager.

This chapter contains the following topics:

- Which Deployment Is Suitable For Your Organization
- Scenario A: Single-hop DMZ Deployment
- Scenario B: Single-hop DMZ Deployment with SecurID Integration
- Scenario C: Double-hop DMZ Deployment

Which Deployment Is Suitable For Your Organization

MetaFrame Secure Access Manager provides secure, single-point access over the Internet to a wide range of internal and external information resources, including applications, data sources, documents, Web content and services. With minimal effort, IT administrators can serve the entire enterprise to a browser, tailored to each user's needs, with fully secure connectivity, over the Internet.

If your enterprise network contains an access center running on MetaFrame Secure Access Manager, you can deploy Secure Gateway to provide secure Internet access to any published resource available through the access center. Published resources include Web sites, internal Web servers, resources published on a server farm, and so on.

In such deployments, the Secure Gateway works with the Logon Agent to provide authentication, authorization, and redirection to the access center.

The following section evaluates recommended topologies for deploying the Secure Gateway with MetaFrame Secure Access Manager.

Single-hop DMZ Deployment

In this configuration, the Secure Gateway provides secure access to an access center running MetaFrame Secure Access Manager. Users connect to the Secure Gateway and upon authentication are allowed to access content, internal Web servers, and published resources aggregated through the access center.

If you choose to integrate SecurID authentication, users are required to enter valid domain and RSA SecurID credentials.

In this configuration, the firewall facing the Internet has port 443 open. The firewall between the DMZ and the secure network has ports 443, 80, 1494 (if accessing published resources), and UDP (User Datagram Protocol) port 5500 (for SecurID authentication) open.

Why You Would Select this Deployment

Deploy the Secure Gateway in this configuration if your network contains a single DMZ segment. This configuration is the simplest deployment and provides a reasonable level of security that meets the requirements of most enterprises.

Double-hop DMZ Deployment

Deploy the Secure Gateway in this configuration if your network contains a double-hop DMZ. In this configuration, the Secure Gateway is installed on a stand-alone server in the first DMZ segment. The firewall between the first DMZ segment and the Internet has port 443 open.

The Logon Agent and the Secure Gateway Proxy are installed on separate servers in the second DMZ segment. The servers running MetaFrame Secure Access Manager and MetaFrame Presentation Server are located within the secure network. The firewall between the first and second DMZ segments has ports 80 and 443 open.

Users connect to the server running the Secure Gateway in the first DMZ segment. The Logon Agent is responsible for user authentication and authorization. The Secure Gateway Proxy is responsible for relaying all data exchanged between the server running the Secure Gateway and servers in the secure network. The firewall between the second DMZ segment and the secure network has ports 80, 443, and 1494 open.

Why You Would Select this Deployment

Citrix recommends deploying the Secure Gateway in this configuration if your network contains a double-hop DMZ. It provides the maximum protection, as an attacker would need to penetrate multiple security zones to reach servers in the secure network.

If the resources aggregated through MetaFrame Secure Access Manager are extremely sensitive and require high level of security, then you should choose this configuration.

Scenario A: Single-hop DMZ Deployment

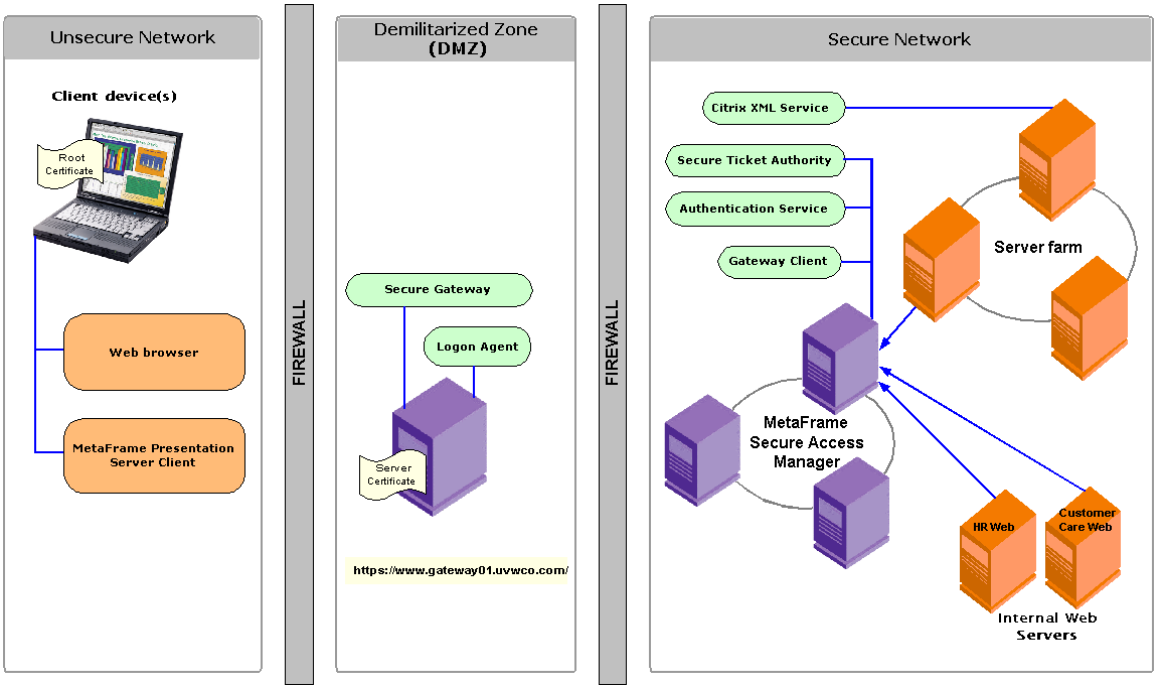
Consider the example of the company, UVWCo Inc. that recently purchased MetaFrame Secure Access Manager, Version 2.0.

The company licensed MetaFrame Presentation Server 3.0 for use in its enterprise network. The Customer Care department deployed MetaFrame Presentation Server in its enterprise network and employees are able to access published resources on the LAN.

They also deployed MetaFrame Secure Access Manager to create an access center that aggregates content from departmental Web servers as well as allow access to resources published on their server farms.

Because they have a large percentage of mobile workers, they now want to deploy the Secure Gateway to provide secure Internet access to the access center.

The company's security and network engineers in consultation with Citrix Consulting Services recommended that the company deploy the Secure Gateway as described in the following diagram.



This illustration shows a typical Secure Gateway deployment used to secure an access center that aggregates content available on internal Web servers and published applications within a server farm. The unsecure network contains a client device(s) running a Web browser and MetaFrame Presentation Server Client, the demilitarized zone contains the Secure Gateway and Logon Agent components, and the secure network contains servers running MetaFrame Secure Access Manager, internal Web servers, and a server farm. MetaFrame Secure Access Manager runs the Secure Ticket Authority, Authentication Service, and Gateway Client. A server within the server farm runs the Citrix XML Service. The content from the internal Web servers and server farm is aggregated by MetaFrame Secure Access Manager. A firewall separates the unsecure network from the demilitarized zone and a second firewall separates the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate machines to enable secure communications.

The security analyst recommended purchasing a single server certificate from a commercial CA to install on the server running the Secure Gateway. The analyst also concluded that it was unnecessary to secure the communication link between the servers running the Secure Gateway and the Authentication Service.

In this network topology, the secure enterprise network is separated from the Internet by a single DMZ segment.

The enterprise network contains servers running MetaFrame Secure Access Manager, a Human Resources Web server, a Customer Care Web server, and a server farm. The firewall separating the secure network from the DMZ has ports 80, 443, and 1494 open.

The DMZ contains a single server running the Secure Gateway and the Logon Agent. The DMZ is separated from the Internet by a firewall that has port 443 open.

Mobile workers carry notebook PCs running a 32-bit Windows operating system, Internet Explorer 5.5 or later, and the MetaFrame Presentation Server Client for 32-bit Windows.

The following sections describe the steps required to deploy the Secure Gateway in the above usage scenario.

Printing and Completing the Pre-installation Checklist

Print and complete the *Secure Gateway Pre-installation Checklist*, available from the Documentation Center.

Doing so ensures you complete pre-installation tasks and have configuration information at hand when you are installing Secure Gateway components.

Setting Up and Testing an Access Center

It is assumed that your enterprise network contains a server farm, correctly configured and accessible from the LAN. The steps below are a list of tasks you need to complete on the server running MetaFrame Secure Access Manager:

1. Install and configure MetaFrame Secure Access Manager on a server(s) in the enterprise network.
2. Create an access center.
3. Configure the access center to include published resources from one or more server farms.
4. Configure the access center to allow external access to internal Web servers through the Secure Gateway.
5. Add one or more instances of the Website Viewer CDA to view an internal Web server on the access center pages.
6. Log on to the access center from the LAN and ensure everything works correctly.

For detailed instructions about these steps, see the *MetaFrame Secure Access Manager Administrator's Guide*, available from the Support area of the Citrix Web site at http://www.citrix.com/.

Installing the Secure Gateway and Logon Agent

Per the recommended deployment scenario, the Secure Gateway and the Logon Agent are installed on a single server in the DMZ. The instructions below guide you through installation and configuration of these components.

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Gateway**. The installation wizard is launched and after a brief interval during which the installer checks the server for installed applications.
4. In the **Installation Mode** section, select **Secure Gateway Service**.
5. In the **Citrix MetaFrame products to secure** section, select **MetaFrame Secure Access Manager and MetaFrame XP Server**. Click **Next**.
6. Under **Logon Agent installation mode**, select **Basic**. Click **Next**.
7. View the information specific to the component you are installing and click **Next**.
8. Review the information in the **Select Features** dialog box and click **Next**.
9. Click through remaining prompts until the installation begins.

When the installation is complete, configuration wizards for the Logon Agent and the Secure Gateway, in that order, are launched.

Configuring the Logon Agent

When installation of Secure Gateway components is complete, the Logon Agent Configuration wizard starts automatically.

To configure the Logon Agent

1. In the **Select configuration level** screen, select **Advanced**.
2. In the **Authentication Service (AS) details** screen, enter the following information:

   FQDN: Enter the fully qualified domain name of the server running the Authentication Service; for example, accesscenter01.uvwco.com.

   Path: Specify the default path and file for the Authentication Service. This is typically /*accesscenter*/AuthService/AuthService.asmx, where *accesscenter* is the name of the access center you created on the server running MetaFrame Secure Access Manager.

   Important If the name of the access center contains a space, you must replace the space with the characters "%20" in the **Path** field. For example, if you called your access center "My Access Center," enter "/My%20Access%20Center/AuthService/AuthService.asmx" in the **Path** field.

   In the **Communication protocol** section, enter the following values:

   Secured with HTTPS: Clear the check box as communications between the Logon Agent and the Authentication Service is unencrypted.

   TCP Port: Specify the network port on which the Authentication Service can be contacted.

   Use default: Select this check box to use the system default port assignment for the Authentication Service. Click **Next** to proceed with configuration.
3. Select the **Set server's default Web page to point to the Logon Agent** check box to make the Logon Agent page the default Web page on this server. For example, when a user connects to http://www.gateway01.uvwco.com/, the Web page for the Logon Agent is displayed.
4. Click **Finish** to save the configuration settings and exit the Logon Agent Configuration wizard.

If you need to modify configuration parameters for the Logon Agent, run the configuration wizard at a later time by selecting **Start > Programs > Citrix > Secure Gateway > Logon Agent Configuration**.

Redirecting All HTTP 404 Errors to the Logon Agent

When a client session times out, the Secure Gateway redirects the subsequent connection request to the Logon Agent. This generates a 404 error if the Web server running IIS is not setup to redirect the request to the Logon Agent page.

Modify settings on the Web server running IIS and the Logon Agent to ensure that 404 errors are always redirected to the Logon Agent page.

This ensures that invalid requests to unknown or invalid URLs directed at the Logon Agent are handled in a graceful manner. In this case, instead of being presented with a "404 - Page Not Found" error, the user will be redirected to the Logon Agent page.

To configure a custom HTTP Error 404 Handler

1. In the IIS Service Manager snap-in, right-click **Default Web Site** and click **Properties**.
2. In the **Default Web Site Properties** dialog box, click the **Custom Errors** tab.
3. Select the **HTTP Error 404** message and click **Edit Properties**.
4. From the **Message Type** drop-down list, select **URL**.
5. In the **URL** field, enter "/default.asp", if the Logon Agent is the default Web page on this Web server.
6. Click **OK** to save changes.

Important Note that customizing the HTTP 404 error handler as described above does not handle error situations if the client session to the access center is active and the user types an invalid URL.

Configuring the Secure Gateway

When configuration of Logon Agent is complete, the Secure Gateway Service Configuration wizard is launched.

To configure the Secure Gateway

1. On the **Select configuration level** screen, select **Advanced**.
2. On the **Select a server certificate** screen, select the server certificate to associate with the Secure Gateway. Click **Next**.
3. On the **Specify secure protocol parameters** screen, select the secure protocol and cipher suite that the Secure Gateway must use for client connections.
4. On the **Configure inbound client connections** screen:
   - Select the **Monitor all IP addresses** check box
   - Accept the default value 443 as the **TCP port** number

   Doing so configures the Secure Gateway to listen for client connection requests on all IP addresses available on this server.
5. On the **Outbound connections from the Secure Gateway Service** screen, select **No Outbound Restrictions**. Click **Next**.
6. The **Authentication Service (AS) details** screen is populated with the configuration values you entered for the Logon Agent. Click **Next**.
7. The **Secure Ticket Authority (STA) details** screen appears. Click **Add**. On the **STA details** screen enter the following information:
   - **FQDN**: Enter the fully qualified domain name of the server running the STA; for example, accesscenter01.uvwco.com.
   - **Path**: Specify the default path and file for the STA, typically /Scripts/CtxSTA.dll.
   - **ID**: This field is populated automatically when you click **Next**. The configuration tool contacts the server address you specified. The unique identifier is read from the server running the STA if the configuration wizard successfully resolves the address specified. If the STA cannot be contacted, you are prompted to manually enter the ID for the STA.

     Enter the unique string used to identify the STA. Enter a maximum of 16 alphanumeric characters, uppercase only. Spaces, punctuation, and special characters are not allowed.

   In the **Communication protocol** section, enter the following values:
   - Ensure the **Secured with HTTPS** check box is cleared

- Select the **Use default** check box to use the default port assignment for the STA

Click **OK**. Click **Next** to proceed with configuration.

8. On the **Connection parameters** screen, click **Next** to accept default values for connection time-outs and connection limits.
9. On the **Logging Exclusions** screen, click **Add** and enter the IP address(es) of a network device(s), such as load balancers, that you want the Secure Gateway to exclude from its application log.
10. On the **Logging level** screen, click **Next** to accept the default logging level for the Secure Gateway.
11. On the **Enter details of the server running the Logon Agent** screen, select **Installed on this computer**.
12. At this point, entry of configuration values required for Secure Gateway operation is complete. The Secure Gateway must be restarted to reflect changes to its configuration. Select the **Start Secure Gateway Service** check box and click **Finish**.

If you need to modify configuration parameters for the Secure Gateway, run the configuration wizard at a later time by selecting **Start > Programs > Citrix > Secure Gateway > Secure Gateway Service Configuration**.

Ensure that you stop the service before modifying configuration settings.

Checking Client Devices

Ensure the client devices connecting to the Secure Gateway meet the compatibility requirements stated in “If Your Users Are Connecting to an Access Center” on page 42.

Testing Your Deployment

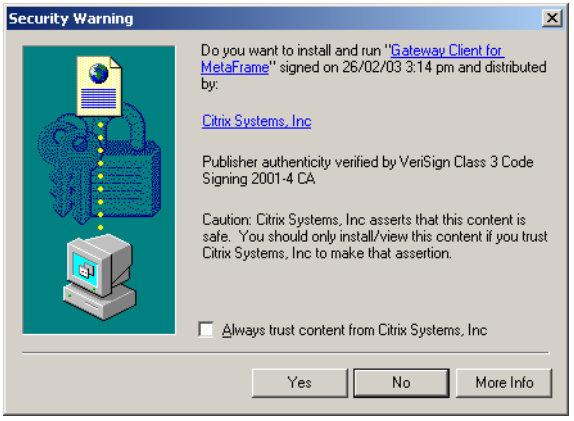
After you complete installing and configuring Secure Gateway components, you are ready to verify your deployment works and is accessible through the Internet.

1. Use a Web browser on a client device to connect to the server running the Secure Gateway; for example, https://www.gateway01.uvwco.com/.
2. Log on using domain credentials.

   A security warning prompting you to install and run the Gateway Client appears.

   Click **Yes**. After a brief interval, the access center page appears.

Important Citrix recommends that you ensure the Gateway Client is a genuine copy signed by Citrix Systems, Inc. before you agree to download it. Click **More Info** in the **Security Warning** dialog box for details. If in doubt about its authenticity, click **No**. For instructions about using the Gateway Client, see "Using the Gateway Client" on page 130.



*This illustration shows the **Security Warning** dialog box associated with the Gateway Client.*

3. Check that you are able to access Web content and published resources.

If you encounter problems loading the access center page, try working your way through the deployment steps to determine the problem.

You can run the Secure Gateway Diagnostics tool by clicking **Start > Programs > Citrix > Secure Gateway > Secure Gateway Diagnostics**. This utility contacts all servers running Secure Gateway components and generates a report containing configuration and status information for each component. See "Viewing a Secure Gateway Diagnostics Report" on page 126 for information about using the Secure Gateway Diagnostics tool.

The Secure Gateway event log is another good source of information. To access the event log, click **Start > Programs > Citrix > Secure Gateway > Secure Gateway Management Console**. You may be able to trace the cause of the problem by referring to the error messages in Appendix A.

Scenario B: Single-hop DMZ Deployment with SecurID Integration

The same company, UVWCo Inc. deployed MetaFrame Secure Access Manager and created an executive access center for its management staff who need 24-hour access to inventory, sales, and financial data.

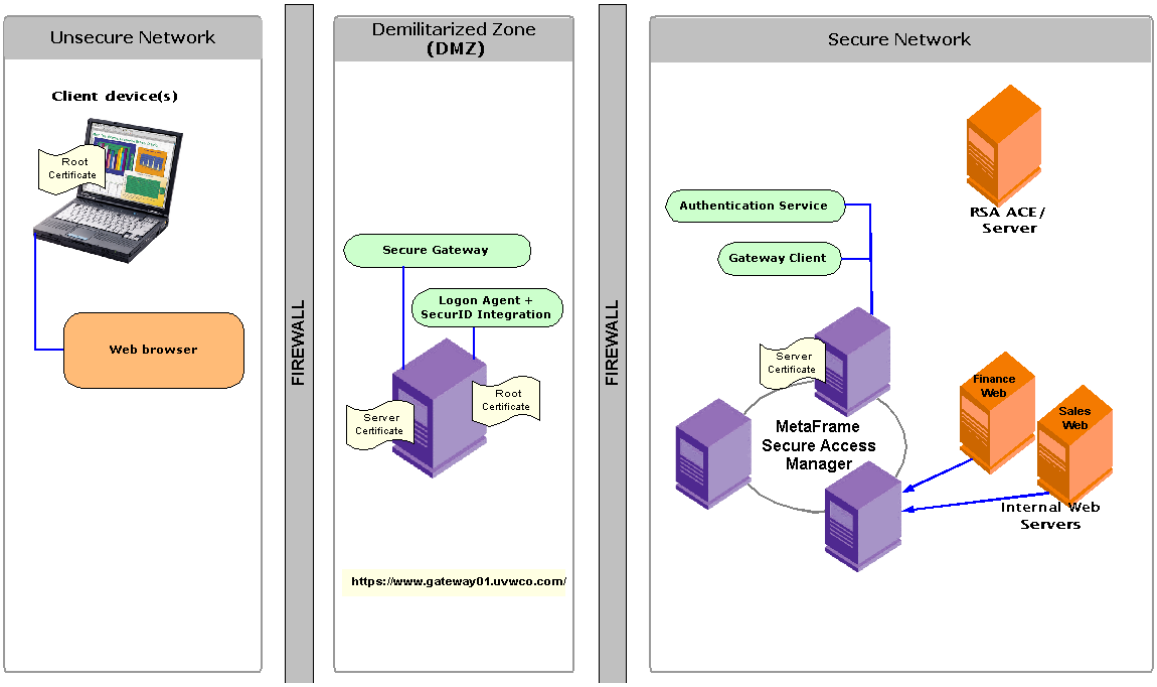
Restricted access to such data and reports is available to executive staff who connect to the access center through the LAN. Content from Web sites of analysts such as Gartner and META groups is aggregated through the access center called UVWCo_Execs.

The executives do not need access to published resources through the access center, so server farms are not aggregated through the UVWCo_Execs access center.

The company's security and network engineers in consultation with Citrix Consulting Services recommended that the company deploy the Secure Gateway for secure Internet access to the UVWCo_Execs access center.

Recommendations include augmenting security using the following measures:

- Secure links between the servers running the Secure Gateway and the Authentication Service
- Integrate RSA SecurID authentication with the Secure Gateway



This illustration shows a typical Secure Gateway and SecurID deployment used to secure MetaFrame Secure Access Manager. The unsecure network contains a client device(s) running a Web browser, the demilitarized zone contains the Secure Gateway Logon Agent, and SecurID Integration components, and the secure network contains servers running MetaFrame Secure Access Manager, internal Web servers, and an RSA/ACE Server. MetaFrame Secure Access Manager runs the Authentication Service and Gateway Client. The content from the internal Web servers is aggregated by MetaFrame Secure Access Manager. A firewall separates the unsecure network from the demilitarized zone and a second firewall separates the demilitarized zone from the secure network. Root and server certificates are installed on the appropriate machines to enable secure communications.

In this network topology, the secure enterprise network is separated from the Internet by a single DMZ segment.

The enterprise network contains servers running MetaFrame Secure Access Manager, a finance Web server, a Sales and Marketing Web server, and an RSA ACE/Server. The firewall separating the secure network from the DMZ has ports 80 and 443 open. The UDP port 5500 is also open to allow communications between the RSA ACE Agent and the RSA ACE/Server located in the secure network.

The DMZ contains a single server running the Secure Gateway and the Logon Agent. The DMZ is separated from the Internet by a firewall that has port 443 open.

Executive staff carry an RSA SecurID token and notebook PCs running a 32-bit Windows operating system, Internet Explorer 5.5 or later, and the MetaFrame Presentation Server Client for 32-bit Windows.

The following sections contain step-by-step instructions to deploy the Secure Gateway in the above usage scenario.

Printing and Completing the Pre-installation Checklist

Print and complete the *Secure Gateway Pre-installation Checklist*, available from the Documentation Center.

Doing so ensures you complete pre-installation tasks and have configuration information at hand when you are installing Secure Gateway components.

Setting Up and Testing the Access Center

It is assumed that your enterprise network contains a server farm, correctly configured and accessible from the LAN. The steps below are a list of tasks you need to complete on the server running MetaFrame Secure Access Manager.

1. Install and configure MetaFrame Secure Access Manager on a server in the enterprise network.
2. Create a new access center; for example, UVWCo_Execs.
3. Configure the access center to allow external access to internal Web servers through the Secure Gateway.
4. Add one or more instances of the Website Viewer CDA to view an internal Web server on the access center page.
5. If you are securing communications between the Secure Gateway and the Authentication Service, ensure a server certificate is installed on the server running the Authentication Service.
6. Log on to the access center from the LAN and ensure you can access the appropriate information from within the secure network.

For detailed instructions about performing these tasks, see the *MetaFrame Secure Access Manager Administrator's Guide*, available from the Support area of the Citrix Web site at http://www.citrix.com/.

Testing RSA SecurID Authentication on the LAN

Ensure that authentication works when you contact the RSA ACE/Server from the RSA ACE Agent. The RSA ACE Agent must be installed on the server reserved for Logon Agent installation.

Tip You can run the **Test Authentication** utility available with RSA ACE Agent software by selecting **Start > Programs > RSA ACE Agent > Test Authentication**.

Installing the Secure Gateway and Logon Agent

Per the recommended deployment scenario, the Secure Gateway and the Logon Agent are installed on the same server in the DMZ. The instructions below guide you through installation and configuration of these components.

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Gateway**. The installation wizard is launched and after a brief interval during which the installer checks the server for installed applications, the **Select Components** dialog box appears.
4. In the **Installation Mode** section, select **Secure Gateway Service**.
5. In the **Citrix MetaFrame products to secure** section, select **MetaFrame Secure Access Manager only**. Click **Next**.
6. Under **Logon Agent installation mode**, select **RSA SecurID Integration**. Click **Next**.
7. Read and accept the license agreement and click **Next**.
8. View information specific to the component you are installing and click **Next**.
9. Review the information in the **Select Features** dialog box and click **Next**.
10. Click through remaining prompts until the installation begins.

    When the installation is complete, configuration wizards for the Logon Agent and the Secure Gateway, in that order, are launched.

Configuring the Logon Agent

The Logon Agent Configuration wizard is launched when the installation of the selected Secure Gateway components is complete.

To configure the Logon Agent

1. From the **Select configuration level** screen, select **Advanced**.
2. From the **Authentication Service (AS) details** screen, enter the following information:
   - **FQDN**: Enter the fully qualified domain name of the server running the Authentication Service; for example, accesscenter01.uvwco.com.

- **Path**: Specify the default path and file for the Authentication Service. This is typically /*AccessCenter*/AuthService/AuthService.asmx, where *AccessCenter* is the name of the access center you created on the server running MetaFrame Secure Access Manager.

Important If the name of the access center contains a space, you must replace the space with the characters "%20" in the **Path** field. For example, if you called your access center "My Access Center," enter "/My%20Access%20Center/AuthService/AuthService.asmx" in the **Path** field.

In the **Communication protocol** section, enter the following values:

- Select the **Secured with HTTPS** check box to encrypt data exchanged between the Logon Agent and the Authentication Service using SSL
- Select the **Use default** check box

Click **Next** to proceed with configuration.

3. Select the **Set server's default Web page to point to the Logon Agent** check box to make the Logon Agent page the default Web page on this server. For example, when a user connects to https://www.gateway01.uvwco.com/, the Web page for the Logon Agent is displayed.
4. Click **Finish** to save these configuration settings and exit the Logon Agent Configuration wizard.

If you need to modify configuration parameters for the Logon Agent at a later time, run the configuration wizard by selecting **Start > Programs > Citrix > Secure Gateway > Logon Agent Configuration**.

Redirecting All HTTP 404 Errors to the Logon Agent

When a client session times out, the Secure Gateway redirects the subsequent connection request to the Logon Agent. This generates a 404 error if the Web server running IIS is not configured to redirect the request to the Logon Agent page.

Citrix recommends that you modify settings on the IIS Web server hosting the Logon Agent to ensure that 404 errors are always redirected to the Logon Agent page.

This ensures that invalid requests to unknown or invalid URLs directed at the Logon Agent are handled in a graceful manner. In this case, instead of being presented with a "404 - Page Not Found" error, the user will be redirected to the Logon Agent page.

To configure a custom HTTP Error 404 Handler

1. In the IIS Service Manager snap-in, right-click **Default Web Site** and click **Properties**.
2. In the **Default Web Site Properties** dialog box, click the **Custom Errors** tab.
3. Select the **HTTP Error 404** message and click **Edit Properties**.
4. From the **Message Type** drop-down list, select **URL**.
5. Enter "/default.asp" in the **URL** field if the Logon Agent is the default Web page on this Web server.
6. Click **OK** to save changes.

Important Note that customizing the HTTP 404 error handler as described above does not handle error situations if the client session to the access center is active and the user types an invalid URL.

Configuring the Secure Gateway

The Secure Gateway Service Configuration wizard is launched when configuration of the Logon Agent is complete.

To configure the Secure Gateway

1. On the **Select configuration level** screen, select **Advanced**.
2. On the **Select a server certificate** screen, select the server certificate to associate with the Secure Gateway. Click **Next**.
3. On the **Specify secure protocol parameters** screen, select the **secure protocol** and **cipher suite** that the Secure Gateway must use for client connections.
4. On the **Configure inbound client connections** screen:
   - Select the **Monitor all IP addresses** check box
   - Accept the default value of **443** as the **TCP port** number

   Doing so configures the Secure Gateway to listen for client connection requests on all IP addresses available on this server.
5. On the **Outbound connections from the Secure Gateway Service** screen, select **No outbound traffic restrictions** and click **Next**.
6. The **Authentication Service (AS) details** screen is populated with the configuration values you entered for the Logon Agent. Click **Next**.
7. On the **Connection parameters** screen, click **Next** to accept the default values for connection timeouts and connection limits.
8. On the **Logging Exclusions** screen, click **Add** and enter the IP address(es) of a network device(s), such as load balancers, that you want the Secure Gateway to exclude from its application log.
9. On the **Logging level** screen, click **Next** to accept the default logging level for the Secure Gateway.
10. On the **Enter details of the server running the Logon Agent** screen, select **Installed on this computer**.
11. At this point, entry of configuration values required for Secure Gateway operation is complete. The Secure Gateway must be restarted to save configuration values to the Windows registry. Select the **Start Secure Gateway Service** check box and click **Finish**.

If you need to modify configuration parameters for the Secure Gateway at a later time, run the configuration wizard by selecting **Start > Programs > Citrix > Secure Gateway > Secure Gateway Service Configuration**.

Checking Client Devices

Ensure client devices connecting to the Secure Gateway meet the compatibility requirements stated in "If Your Users Are Connecting to an Access Center" on page 42.

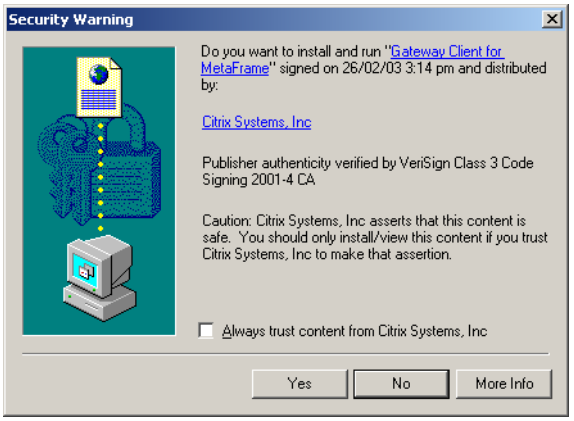
Testing Your Deployment

After you complete the installation and configuration of Secure Gateway components, you need to test that your deployment works and is accessible through the Internet.

1. Use a Web browser on a client device to connect to the server running the Secure Gateway; for example, https://www.gateway01.uvwco.com/.
2. Log on using domain and RSA SecurID credentials. A security warning prompting you to install and run the Gateway Client appears.

   Click **Yes**. After a brief interval, the access center page appears.

Important Citrix recommends that you ensure the Gateway Client is a genuine copy signed by Citrix Systems, Inc. before you agree to download it. Click **More Info** in the **Security Warning** dialog box for details. If in doubt about its authenticity, click **No**. For instructions about using the Gateway Client, see "Using the Gateway Client" on page 130.



*This illustration shows the **Security Warning** dialog box associated with the Gateway Client.*

3. Verify that you are able to access Web content and published resources.

If you encounter problems loading the Web page for the access center, try working your way through the deployment steps to figure out the problem.

You can run the Secure Gateway Diagnostics tool by clicking **Start > Programs > Citrix > Secure Gateway > Secure Gateway Diagnostics**. This utility contacts all servers running Secure Gateway components and generates a report containing configuration and status information for each component. See "Viewing a Secure Gateway Diagnostics Report" on page 126 for information about using the Secure Gateway Diagnostics tool.

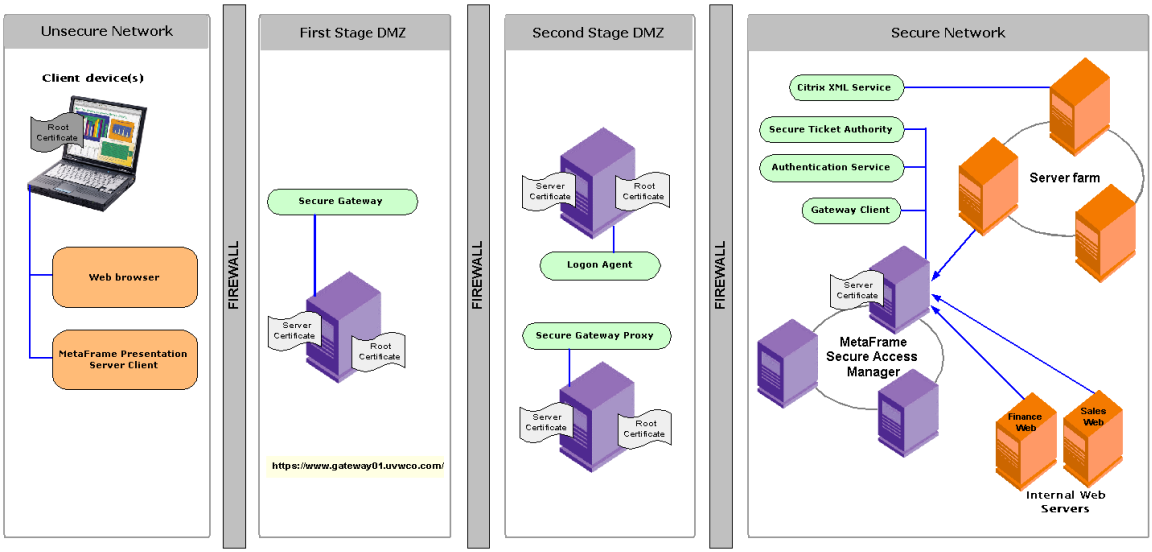
The Secure Gateway event log is another good source of information. To access the event log, click **Start > Programs > Citrix > Secure Gateway > Secure Gateway Management Console**. You may be able to trace the cause of the problem by referring to the error messages in Appendix A.

Scenario C: Double-hop DMZ Deployment

UVWCo, Inc. deployed MetaFrame Secure Access Manager for access to internal Web servers and resources published on a server farm.

They plan to deploy the Secure Gateway to provide secure Internet access to resources aggregated through MetaFrame Secure Access Manager.

The security analyst consulted recommended setting up a double-hop DMZ between the Internet and the enterprise network, and securing communications between all Secure Gateway components.



This illustration shows a typical double-hop Secure Gateway deployment used to secure an access center that aggregates content available on internal Web servers and published applications within a server farm. The unsecure network contains notebook PCs running a 32-bit Windows operating system, Internet Explorer 5.5, and the MetaFrame Presentation Server Client for 32-bit Windows.

The first stage of the DMZ contains the Secure Gateway, the second stage of the DMZ contains the Logon Agent and the Secure Gateway Proxy, and the secure network contains servers running MetaFrame Secure Access Manager, internal Web servers, and a server farm. MetaFrame Secure Access Manager runs the Secure Ticket Authority, Authentication Service, and Gateway Client. A server within the server farm runs the Citrix XML Service. The content from the internal Web servers and server farm is aggregated by MetaFrame Secure Access Manager. A firewall separates the unsecure network from the first stage of the DMZ, a second firewall separates the first stage of the DMZ from the second stage of the DMZ, and a third firewall separates the second stage of the DMZ from the secure network. Root and server certificates are installed on the appropriate machines to enable secure communications.

One of the servers running MetaFrame Secure Access Manager is a secure server. The firewall separating the secure network from the second DMZ segment has ports 80, 443, and 1494 open.

The second DMZ segment contains a secure server running the Secure Gateway Proxy and a secure Web server running the Logon Agent. The firewall separating the first DMZ segment from the second has port 443 open. If the communications link between the Secure Gateway and the Secure Gateway Proxy is not secured, open port 1080 on the firewall between the first and second DMZ segments.

The following sections describe typical steps required to deploy the Secure Gateway in the above usage scenario.

Printing and Completing the Pre-installation Checklist

Print and complete the *Secure Gateway Pre-installation Checklist*, available from the Documentation Center.

Doing so ensures you complete pre-installation tasks and have configuration information at hand when you are installing Secure Gateway components.

Setting Up and Testing an Access Center

It is assumed that your enterprise network contains a server farm, correctly configured and accessible from the LAN. The steps below are a list of tasks you need to complete on the server running MetaFrame Secure Access Manager:

1. Install and configure MetaFrame Secure Access Manager on a server in the enterprise network.
2. Create an access center on the server running MetaFrame Secure Access Manager.
3. Configure the access center to include published resources from one or more server farms.
4. Add an appropriate CDA to the access center to enable users to view published resources available.
5. Configure the access center to allow external access to internal Web servers through the Secure Gateway.
6. Add one or more instances of the Website Viewer CDA to view an internal Web server on the access center page.
7. Configure the Secure Ticket Authority. The STA issues “ICA tickets” in response to connection requests for published resources. These session tickets form the basis of authentication and authorization for access to published resources aggregated in the access center.
8. If you are securing communications between the Secure Gateway and the Authentication Service, ensure a server certificate is installed on the server running the Authentication Service.
9. Log on to the access center from the LAN and ensure everything works correctly.

For detailed instructions about these tasks, see the *MetaFrame Secure Access Manager Administrator’s Guide*, available from the Support area of the Citrix Web site at http://www.citrix.com/.

Installing and Configuring the Logon Agent

Per the recommended deployment scenario, the Logon Agent is installed on a stand-alone server in the second DMZ segment. The instructions describe installation and configuration of the Logon Agent.

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Gateway**. The installation wizard is launched and after a brief interval during which the installer checks the server for installed applications, the **Select Components** dialog box appears.
4. In the **Installation Mode** section, select **Secure Gateway Service**.
5. In the **Citrix MetaFrame products to secure** section, select **MetaFrame Secure Access Manager and MetaFrame XP Server**. Click **Next**.
6. Under **Logon Agent installation mode**, select **Basic**. Click **Next**.
7. Read and accept the license agreement and click **Next**.
8. View information specific to the component you are installing and click **Next**.
9. In the **Select Features** dialog box, click the entry for the Logon Agent and select **Will be installed on local hard drive** from the menu displayed. Click the entry for the Secure Gateway Service and Tools and select **Entire feature will be unavailable**.
10. Click **Next**.
11. Click through remaining prompts until the installation begins.

    When the installation is complete, the configuration wizard for the Logon Agent is launched.

To configure the Logon Agent

1. On the **Select configuration level** screen, select **Advanced**.
2. On the **Authentication Service (AS) details** screen, enter the following information:
   - **FQDN**: Enter the fully qualified domain name of the server running the Authentication Service; for example, accesscenter01.uvwco.com.
   - **Path**: Specify the default path and file for the Authentication Service, typically /*AccessCenter*/AuthService/AuthService.asmx, where *AccessCenter* is the name of the access center you created on the server running MetaFrame Secure Access Manager.

Important If the name of the access center contains a space, you must replace the space with the characters "%20" in the **Path** field. For example, if you called your access center "My Access Center," enter "/My%20Access%20Center/AuthService/AuthService.asmx" in the **Path** field.

In the **Communication protocol** section, enter the following values:

- **Secured with HTTPS**: Select this check box to secure the communications link between the Logon Agent and the Authentication Service.
- **TCP Port**: Specifies the network port on which the Authentication Service can be contacted.
- **Use default**: Select this check box to use the system default port assignment for the Authentication Service. Click **Next** to proceed with configuration.

3. Select the **Set server's default Web page to point to the Logon Agent** check box to make the Logon Agent page the default Web page on this server. For example, when a user connects to http://www.gateway01.uvwco.com/, the Web page for the Logon Agent is displayed.
4. Click **Finish** to save the configuration settings and exit the Logon Agent Configuration wizard.

If you need to modify configuration parameters for the Logon Agent at a later time, run the configuration wizard by selecting **Start > Programs > Citrix > Secure Gateway > Logon Agent Configuration**.

Redirecting All HTTP 404 Errors to the Logon Agent

When a client session times out, the Secure Gateway redirects the subsequent connection request to the Logon Agent. This generates a 404 error if the Web server running IIS is not setup to redirect the request to the Logon Agent page.

Citrix recommends that you modify settings on the Web server running IIS hosting the Logon Agent to ensure that 404 errors are always redirected to the Logon Agent page.

This ensures that invalid requests to unknown or invalid URLs directed at the Logon Agent are handled in a graceful manner. In this case, instead of being presented with a "404 - Page Not Found" error, the user will be redirected to the Logon Agent page.

To configure a custom HTTP Error 404 Handler

1. In the IIS Service Manager snap-in, right-click **Default Web Site** and click **Properties**.
2. In the **Default Web Site Properties** dialog box, click the **Custom Errors** tab.

3. Select the **HTTP Error 404** message and click **Edit Properties**.
4. From the **Message Type** drop-down list, select **URL**.
5. Enter "/default.asp" in the **URL** field if the Logon Agent is the default Web page on this Web server.
6. Click **OK** to save the changes.

Important Note that customizing the HTTP 404 error handler as described above does not handle error situations if the client session to the access center is active and the user types an invalid URL.

Installing and Configuring the Secure Gateway Proxy

Install the Secure Gateway Proxy on a stand-alone server in the second DMZ segment. If you are securing communications between the Secure Gateway and the Secure Gateway Proxy, ensure you install a server certificate on the server running the Secure Gateway Proxy.

To install the Secure Gateway Proxy

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Gateway**. The installation wizard is launched and after a brief interval during which the installer checks the server for installed applications, the **Select Components** dialog box appears.
4. In the **Installation mode** section, select **Secure Gateway Proxy**.
5. In the **Citrix MetaFrame products to secure** section, select **MetaFrame Secure Access Manager and MetaFrame Server**. Click **Next**.
6. Read and accept the license agreement and click **Next**.
7. View information specific to the component you are installing and click **Next**.
8. Review information in the **Select Features** dialog box and click **Next**.
9. Click through remaining prompts until the installation begins.

When the installation is complete, the configuration wizard is launched.

To configure the Secure Gateway Proxy

1. On the **Select configuration level** screen, select **Advanced** and select the **Secure traffic between the Secure Gateway Service and the Secure Gateway Proxy** check box.

2. On the **Select a server certificate** screen, select the server certificate to associate with the Secure Gateway Proxy. Click **Next**.
3. On the **Specify secure protocol parameters** screen, click **Next** to accept default values for the **secure protocol** and **cipher suite** that the Secure Gateway Proxy uses for client connections.
4. On the **Configure inbound client connections** screen:
   - Select the **Monitor all IP addresses** check box
   - Accept the default value of **443** as the **TCP port** number

   Doing so configures the Secure Gateway Proxy to listen for client connection requests on all IP addresses available on this server.
5. On the **Configure outbound connections from the Secure Gateway Proxy** screen, select **No outbound traffic restrictions**.
6. On the **Connection parameters** screen, click **Next** to accept default values for connection time-outs and connection limits.
7. On the **Logging Exclusions** screen, click **Add** and enter the IP address(es) of a network device(s), such as load balancers, that you want the Secure Gateway Proxy to exclude from its application log.
8. In the **Logging level** screen, click **Next** to accept the default logging level for the Secure Gateway Proxy.
9. At this point, entry of configuration values required for the Secure Gateway Proxy operation is complete. The Secure Gateway Proxy must be restarted to reflect the changes to its configuration. Select the **Start Secure Gateway Proxy** check box, and click **Finish**.

If you need to modify configuration parameters for the Secure Gateway Proxy at a later time, run the configuration wizard by selecting **Start > Programs > Citrix > Secure Gateway > Secure Gateway Service Configuration**.

Installing and Configuring the Secure Gateway

Install the Secure Gateway on a stand-alone server in the first DMZ segment.

To install the Secure Gateway

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Gateway**. The installation wizard is launched and after a brief interval during which the installer checks the server for installed applications, the **Select Components** dialog box appears.
4. In the **Installation mode** section, select **Secure Gateway Service**.
5. In the **Citrix MetaFrame products to secure** section, select **MetaFrame Secure Access Manager and MetaFrame XP Server**. Click **Next**.
6. Read and accept the license agreement and click **Next**.
7. View information specific to the component you are installing and click **Next**.
8. In the **Select Features** dialog box, click the entry for the Secure Gateway Service and Tools and select **Will be installed on local hard drive** from the menu displayed. Click the entry for the Logon Agent, select **Entire feature will be unavailable** from the menu displayed, and click **Next**.
9. Click through remaining prompts until the installation begins.

When the installation is complete, the Secure Gateway Service Configuration wizard is launched.

To configure the Secure Gateway

1. On the **Select configuration level** screen, select **Advanced**.
2. On the **Select a server certificate** screen, select the server certificate to associate with the Secure Gateway. Click **Next**.
3. On the **Specify secure protocol parameters** screen, click **Next** to accept default values for the **secure protocol** and **cipher suite** that the Secure Gateway uses for client connections.
4. On the **Configure inbound client connections** screen:
   - Select the **Monitor all IP addresses** check box
   - Accept the default value of **443** as the **TCP port** number

   Doing so configures the Secure Gateway to listen for client connection requests on all IP addresses available on this server.

5. Select **Use the Secure Gateway Proxy** as the outbound connection setting. Enter the following details for the Secure Gateway Proxy:
   - **FQDN**: Enter the fully qualified domain name of the server running the Secure Gateway Proxy; for example, gwyproxy01.uvwco.com.
   - **Secured:** Select this check box to encrypt communications between the Secure Gateway and the Secure Gateway Proxy.
   - **Use default**: Select this check box to use the default TCP port assignment when connecting to a secure server.

   Click **Next**.
6. On the **Authentication Service (AS) details** screen, enter the following information:
   - **FQDN**: Enter the fully qualified domain name of the server running the Authentication Service; for example, accesscenter01.uvwco.com.
   - **Path**: Specify the default path and file for the Authentication Service, typically /*AccessCenter*/AuthService/AuthService.asmx, where *AccessCenter* is the name of the access center you created on the server running MetaFrame Secure Access Manager.

   Important If the name of the access center contains a space, you must replace the space with the characters "%20" in the **Path** field. For example, if you called your access center "My Access Center," enter "/My%20Access%20Center/AuthService/AuthService.asmx" in the **Path** field.

   In the **Communication protocol** section, enter the following values:
   - Select the **Secured with HTTPS** check box to encrypt data exchanged between the Secure Gateway and the Authentication Service using SSL
   - Select the **Use default** check box

   Click **Next** to proceed with configuration.
7. The **Secure Ticket Authority (STA) details** screen appears. Click **Add**.
8. In the **STA details** screen, enter the following information:
   - **FQDN**: Enter the fully qualified domain name of the server running the STA, for example, sta01.uvwco.com.
   - **Path**: Specify the default path and file for the STA. This is typically /Scripts/CtxSTA.dll.

- **ID**: This field is populated automatically when you click **Next**. The configuration tool contacts the server address you specified. The unique identifier is read from the server running the STA if the configuration wizard successfully resolves the address specified. If the STA cannot be contacted, you are prompted to enter the ID for the STA manually.

  Enter the unique string used to identify the STA. Enter a maximum of 16 alphanumeric characters, uppercase only. Spaces, punctuation, and special characters are not allowed.

In the **Communication protocol** section, enter the following values:

- Select the Secured **with HTTPS** check box
- Select the **Use default** check box to use the default port assignment for the STA

Click **OK**.

9. Click **Next** to proceed with configuration.
10. On the **Connection parameters** screen, click **Next** to accept default values for connection time-outs and connection limits.
11. On the **Logging Exclusions** screen, click **Add** and enter the IP address(es) of a network device(s), such as load balancers, that you want the Secure Gateway to exclude from its application log.
12. On the **Logging level** screen, click **Next** to accept the default logging level for the Secure Gateway.
13. In the **Enter details of the server running the Logon Agent**, do the following:
    - For the **Location**, select **Installed on a different computer**
    - In the **Details** section, enter the **FQDN** of the server running the Logon Agent; for example, logonagent.uvwco.com.
    - Select the **Secured with HTTPS** check box
    - Accept the default value of **443** as the **TCP port number**

    Click **Next**.
14. At this point, the entry of configuration values required for Secure Gateway operation is complete. The Secure Gateway must be restarted to reflect changes to its configuration. Select the **Start Secure Gateway Service** check box and click **Finish**.

If you need to modify configuration parameters for the Secure Gateway, run the configuration wizard at a later time by selecting **Start > Programs > Citrix > Secure Gateway > Secure Gateway Service Configuration**.

Checking Client Devices

Ensure that all client devices connecting to the access center meet compatibility requirements stated in "If Your Users Are Connecting to an Access Center" on page 42.

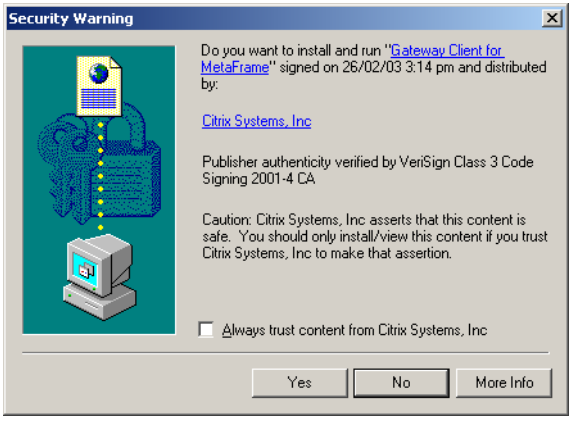
Testing Your Deployment

After you complete installation and configuration of all Secure Gateway components, you need to verify that your deployment works and is accessible through the Internet.

1. Use a Web browser on a client device to connect to the server running the Secure Gateway; for example, https://www.gateway01.uvwco.com/.
2. Log on using domain credentials.
3. A security warning prompting you to install and run the Gateway Client appears.

   Click **Yes**. After a brief interval, the access center page appears.

Important Citrix recommends that you ensure the Gateway Client is a genuine copy signed by Citrix Systems, Inc. before you agree to download it. Click **More Info** in the **Security Warning** dialog box for details. If in doubt about its authenticity, click **No**. For instructions about using the Gateway Client, see "Using the Gateway Client" on page 130.



*This illustration shows the **Security Warning** dialog box associated with the Gateway Client.*

4. Verify that you are able to access internal Web servers and published resources.

If you encounter problems loading the access center page, try working your way through the deployment steps to figure out the problem.

You can run the Secure Gateway Diagnostics tool by clicking **Start > Programs > Citrix > Secure Gateway > Secure Gateway Diagnostics**. This utility contacts all servers running Secure Gateway components and generates a report containing configuration and status information for each component. See "Viewing a Secure Gateway Diagnostics Report" on page 126 for information about using the Secure Gateway Diagnostics tool.

The Secure Gateway event log is another good source of information. To access the event log, click **Start > Programs > Citrix > Secure Gateway > Secure Gateway Management Console**. You may be able to trace the cause of the problem by referring to the error messages in Appendix A.

Deploying Secure Gateway with Server Farms

This chapter provides guidance on selecting a deployment suitable for your organization. It also describes the steps required to deploy the Secure Gateway to provide access to a server farm. This chapter contains the following topics:

- Which Deployment Is Suitable For Your Organization
- Scenario A: Single-hop DMZ Deployment
- Scenario B: Double-hop DMZ Deployment
- Scenario C: Upgrading a Secure Gateway, Version 1.x Deployment

Which Deployment Is Suitable For Your Organization

The foundation of the Citrix MetaFrame Access Suite, MetaFrame Presentation Server is the world's most widely deployed presentation server for centrally managing heterogeneous applications and delivering their functionality as a service to workers, wherever they may be. Designed to enhance Windows 2000 and 2003 Servers, MetaFrame Presentation Server provides the exceptional scalability, interoperability, manageability, flexibility and network leverage that the enterprise requires from an access infrastructure solution, while delivering end-to-end security and measurable business and IT benefits.

If your enterprise network contains a server farm, you can deploy the Secure Gateway to provide secure Internet access to published resources.

In such deployments, the Secure Gateway works with the Web Interface to provide authentication, authorization, and redirection to published resources hosted on a computer running MetaFrame Presentation Server.

The following section evaluates recommended topologies in which you can deploy the Secure Gateway and the Web Interface for access to server farms.

Single-hop DMZ Deployments

Web Interface Located Behind the Secure Gateway in the DMZ

All incoming traffic is intercepted by the Secure Gateway deployed in the DMZ. You can install the Web Interface on the same server as the Secure Gateway, or install it on a separate server. All data exchanged between client devices and the Web Interface is relayed through the Secure Gateway.

The firewall facing the Internet has port 443 open. Users connect to the Secure Gateway using a URL such as https://Secure Gateway FQDN/.

Advantages

The advantages of deploying the Secure Gateway in this configuration are as follows:

- A single server certificate is required on the server running the Secure Gateway and the Web Interface
- A single port, 443, must be opened on the firewall facing the Internet
- The Web Interface cannot be contacted directly from the Internet and is therefore more secure

Disadvantages

Deploying the Secure Gateway in this configuration has the following limitations:

Web Interface Functionality Is Affected. When you deploy the Secure Gateway in this configuration, you lose some of the features available with the Web Interface. These include:

- **Smart Card Authentication** The Secure Gateway negotiates the SSL handshake and terminates the SSL connection before forwarding the client connection request to the Web Interface. Smart card authentication integrated with the Web Interface is unavailable because client certificates are not available to the Web Interface.
- **Firewall and Proxy Settings Requiring Knowledge of the Client IP Address Are Ineffective** All communication from the client device to the Web Interface is proxied through the Secure Gateway. As a result, all client communications to the Web Interface originate from the IP address of the server running the Secure Gateway. Though you can still configure firewall and proxy settings on the Web Interface for specific client address prefixes, these settings must allow for all client communications through the Secure Gateway having this IP address. You will not be able to distinguish between different client devices connecting through the Secure Gateway. For information about these features, see the *Web Interface Administrator's Guide,* available from the Document Center.

Why You Would Select This Deployment

Citrix recommends deploying the Secure Gateway in this configuration if your network is small to medium sized, with a usage profile of hundreds of users. This type of deployment is optimal when users are connecting over the Internet to the Secure Gateway.

If any of the limitations described above are a concern and you have a sizeable user base accessing the Secure Gateway over the LAN, then consider deploying the Web Interface in the configuration described in “The Web Interface Is Located in Parallel to the Secure Gateway” on page 90.

The Web Interface Is Located in Parallel to the Secure Gateway

In this configuration, the Secure Gateway and the Web Interface are installed on separate servers. Users can connect directly to the Web Interface. Alternatively, users can connect to the Secure Gateway which redirects them to the Web Interface.

Citrix recommends securing both servers, that is, installing a server certificate on the servers running the Secure Gateway and the Web Interface. Open port 443 on the firewall facing the Internet.

Users connect directly to the Web Interface, using a URL such as https://Web Interface FQDN/citrix/MetaFrame/. Alternatively, users can connect to the Secure Gateway, with a URL such as https://Secure Gateway FQDN/, which is set up to redirect client connections to the Web Interface.

Why You Would Select This Deployment

You want to use the features available with the Web Interface, including smart card authentication and firewall and proxy settings that depend on knowing the client IP address.

Double-hop DMZ Deployments

Deploy the Secure Gateway in a double-hop DMZ configuration if your DMZ is divided into two segments. In this configuration, the server running the Secure Gateway is in the first DMZ segment. The firewall between the first DMZ segment and the Internet has port 443 open.

The Web Interface and the Secure Gateway Proxy are installed on separate servers in the second DMZ segment. The server farm is located in the secure network. The firewall between the first and second DMZ segments has ports 80 and 443 open.

The Secure Gateway, deployed in the first DMZ segment, is responsible for intercepting all incoming traffic. The Web Interface is responsible for user authentication and authorization. The Secure Gateway Proxy is responsible for relaying all data exchanged between the Secure Gateway and servers in the secure network. The firewall between the second DMZ segment and the secure network has ports 80, 443, and 1494 open.

Why You Would Select This Deployment

Deploy the Secure Gateway in this configuration if your network contains a double-hop DMZ. A double-hop DMZ provides additional protection as an attacker would need to penetrate multiple security zones to reach servers in the secure network.

If the resources accessible through the Secure Gateway are extremely sensitive and require a high level of security, then you should consider this configuration.

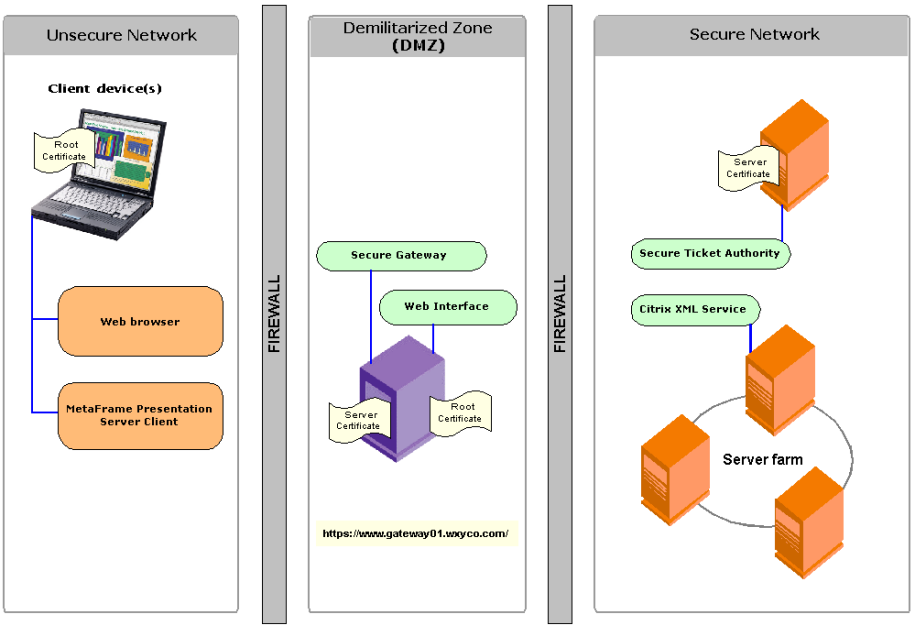
Important The same limitations described in "Web Interface Located Behind the Secure Gateway in the DMZ" on page 88 apply when you deploy the Secure Gateway in a double-hop DMZ configuration.

Scenario A: Single-hop DMZ Deployment

Consider the example of WXYCo Inc., an audit firm that recently purchased licenses for MetaFrame Presentation Server.

The company's employees are financial auditors who visit client sites and conduct financial audits. They use a proprietary, client-server auditing software application, AuditorX. They published AuditorX on computers running MetaFrame Presentation Server. They also deployed the Web Interface for Web access to their published resources. Employees can access AuditorX and other published resources through a Web browser on a client device connected to the LAN.

WXYCo is evaluating the Secure Gateway, which is available to Subscription Advantage subscribers from the Citrix Web site. WXYCo realizes installing the Secure Gateway allows them to provide secure Internet access to published resources on its server farms. Because the workforce is largely mobile, use of the Internet to connect to the enterprise network is expected to dramatically reduce remote access costs.



This diagram illustrates a secure enterprise network separated from the Internet by a single-hop DMZ. The enterprise network contains a server farm and a server running the Secure Ticket Authority (STA). The firewall separating the secure network from the DMZ has ports 80, 443, and 1494 open.

The DMZ contains a single server running the Secure Gateway and the Web Interface. Traffic to the Web Interface is proxied through the Secure Gateway. The Secure Gateway communicates with the Web Interface using HTTP.

The DMZ is separated from the Internet by a firewall that has port 443 open. The mobile workforce carries notebook PCs running a 32-bit Windows operating system, Internet Explorer 5.5, and the MetaFrame Presentation Server Client for 32-bit Windows.

The security analyst consulted recommends securing the communication link between the Secure Gateway and the STA. To this end, the company purchased two server certificates from a commercial CA.

The following sections describe the steps required to deploy the Secure Gateway in this usage scenario.

Printing and Completing the Pre-installation Checklist

Print and complete the *Secure Gateway Pre-installation Checklist*, available from the Documentation Center.

Doing so ensures you complete pre-installation tasks and have configuration information at hand when you are installing Secure Gateway components.

Setting Up and Testing a Server Farm

The steps below provide a list of tasks you need to complete prior to installing and configuring the Secure Gateway.

1. Install and configure a server farm in the enterprise network.
2. Install, configure, and publish applications on the server farm.
3. Connect to the server farm using a client device and ensure you are able to access available published resources.

For detailed instructions about performing these tasks, see the *MetaFrame Presentation Server Administrator's Guide*, available from the Document Center.

Installing and Configuring the STA

The STA is an Internet Server Application Program Interface (ISAPI) DLL, that is loaded and called by Internet Information Services (IIS) when a request for a ticket is received from the Web Interface. The STA issues "session tickets" in response to connection requests for published resources. These session tickets form the basis of authentication and authorization for access to published resources on the server farm. Per the scenario described, the server running the STA must be located in the secure network.

Important If you are securing communications between the Secure Gateway and the STA, ensure you install a server certificate on the server running the STA.

To install the STA

Before installing the STA, verify the server on which you intend to install the STA meets the installation prerequisites specified in "For the Secure Ticket Authority" on page 41.

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Ticket Authority**. The installation program starts. You must complete the following tasks during installation:
   - Read and accept the license agreement.
   - View information specific to the installation of the STA software.
   - Ensure that the STA is installed to the same directory as IIS. By default, the STA is installed to \inetpub\scripts\.

Important Ensure you specify the directory to which you installed IIS as the STA installer does not automatically detect the IIS directory.

The files required for STA operation are installed and the Secure Ticket Authority Configuration wizard is launched.

To configure the STA

1. On the **Select configuration level** screen, select **Advanced**.
2. On the **Configure the Secure Ticket Authority** screen, click **Next** to accept default configuration values for the STA.
3. To use the new configuration settings for the STA, you must restart the World Wide Web Publishing Service. If you prefer to restart the service manually, clear the **Restart the Service** check box.
4. Click **Finish** to exit the STA Configuration wizard.

To change configuration parameters for the STA, run the STA Configuration wizard by selecting **Start > Programs > Citrix > Secure Gateway > Secure Ticket Authority Configuration**.

Important Restart the World Wide Web Publishing Service to allow configuration changes to take effect.

Setting Up and Testing the Web Interface

Per the scenario described, the Web Interface and the Secure Gateway are hosted on the same server in the DMZ. Citrix recommends you install and configure the Web Interface before you install the Secure Gateway.

1. Install the Web Interface on the server reserved for the Secure Gateway and Web Interface.
2. Add and configure a server farm(s) for use with the Web Interface.
3. Use a Web browser on a client device to connect and log on to the Web Interface.
4. Check that you can launch published applications.

For detailed instructions about performing these tasks, see the *Web Interface Administrator's Guide*, available from the Document Center.

Installing and Configuring the Secure Gateway

Per the recommended deployment scenario, the Secure Gateway is installed on the same server as the Web Interface in the DMZ. The instructions below guide you through installation and configuration of the Secure Gateway.

To install the Secure Gateway

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Gateway**. The installation wizard is launched and after a brief interval during which the installer checks the server for installed applications, the **Select Components** dialog box appears.
4. In the **Installation mode** section, select **Secure Gateway Service**.
5. In the **Citrix MetaFrame products to secure** section, select **MetaFrame XP Servers only**. Click **Next**.
6. Read and accept the license agreement and click **Next**.
7. View information specific to the component you are installing and click **Next**.
8. Review information in the **Select Features** dialog box and click **Next**.
9. Click through remaining prompts until installation begins.

When installation is complete, the Secure Gateway Service Configuration wizard is launched.

To configure the Secure Gateway

1. On the **Select configuration level** screen, select **Advanced**.
2. On the **Select a server certificate** screen, select the server certificate to associate with the Secure Gateway. Click **Next**.
3. On the **Specify secure protocol parameters** screen, click **Next** to accept default values for the **secure protocol** and **cipher suite** that the Secure Gateway uses for client connections.
4. On the **Configure inbound client connections** screen:
   - Select the **Monitor all IP addresses** check box
   - Accept the default value of 443 as the **TCP port** number

   Doing so configures the Secure Gateway to listen for client connection requests on all IP addresses available on this server.
5. On the **Outbound connections from the Secure Gateway Service** check box, select **No outbound traffic restrictions**.

6. The **Secure Ticket Authority (STA) details** screen appears. Click **Add**. On the **STA details** screen, enter the following information:

   - **FQDN**: Enter the fully qualified domain name of the server running the STA; for example, sta01.wzyco.com.
   - **Path**: Specify the default path and file for the STA. This is typically /Scripts/CtxSTA.dll.
   - **ID**: This field is populated automatically when you click **Next**. The configuration tool contacts the server address you specified. The unique identifier is read from the server running the STA if the configuration wizard successfully resolves the address specified. If the STA cannot be contacted, you are prompted to enter the ID for the STA manually.

     Enter the unique string used to identify the STA. Enter a maximum of 16 alphanumeric characters, uppercase only. Spaces, punctuation, and special characters are not allowed.

   In the **Communication protocol** section, enter the following values:

   - Select the **Secured with HTTPS** check box.
   - Select the **Use default** check box to use the default port assignment for the STA. Click **OK**.

   Click **Next** to proceed with configuration.

7. On the **Connection parameters** screen, click **Next** to accept the default values for connection time-outs and connection limits.
8. On the **Logging Exclusions** screen, click **Add** and enter the IP address(es) of a network device(s), such as load balancers, that you want the Secure Gateway to exclude from its application log.
9. On the **Logging level** screen, click **Next** to accept the default logging level for the Secure Gateway.
10. On the **Enter details of the server running Web Interface for MetaFrame XP** screen, select **Installed on this computer** as the **Location**.

    Click **Next**.
11. At this point, you completed entry of configuration parameters required for Secure Gateway operation. The Secure Gateway must be restarted to reflect changes to its configuration. Select the **Start Secure Gateway Service** check box and click **Finish**.

If you need to modify configuration parameters for the Secure Gateway Service, run the configuration wizard at a later time by selecting **Start > Programs > Citrix > Secure Gateway > Secure Gateway Service Configuration**.

Configuring the Web Interface to Support the Secure Gateway

You need to configure the Web Interface to interact with Secure Gateway components to provide authentication and authorization functionality. For detailed instructions about configuring the Web Interface to support the Secure Gateway, refer to the *Web Interface Administrator's Guide*, available from the Document Center.

Checking Client Devices

Ensure the client devices connecting to the Secure Gateway meet the compatibility requirements stated in “If Your Users Are Connecting to a Server Farm” on page 43.

Publishing the URL to Log On to the Secure Gateway

Because all traffic to the Web Interface is proxied through the Secure Gateway, users need to type the following URL to access the logon page:

`https://`*`Secure Gateway FQDN`*`/Citrix/MetaFrame/`

where *Secure Gateway FQDN* is the fully qualified domain name for the server running the Secure Gateway. In the case of WXYCo, the URL for the log on page is:

`https://www.gateway01.wzyco.com/Citrix/MetaFrame/`

Inform your users about the new URL they need to enter to access published resources through the Secure Gateway.

Testing Your Deployment

After you complete installation and configuration of the Secure Gateway, you need to test that your deployment works and is accessible through the Internet.

1. Use a Web browser on a client device to connect to the Secure Gateway; for example, https://www.gateway01.wzyco.com/Citrix/MetaFrame/.
2. Log on using domain credentials. After a brief interval, the **Applications** page containing icons for published resources appears.
3. Verify that you are able to launch published applications from this page.

If you encounter problems loading the logon page, try working your way through the deployment steps to figure out the problem.

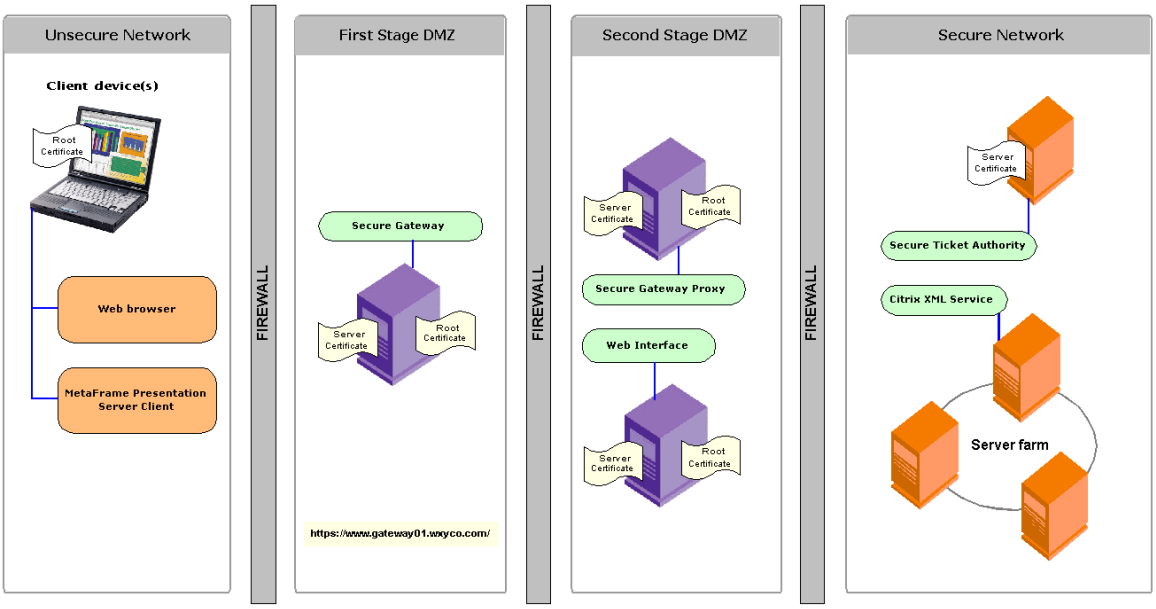
You can run the Secure Gateway Diagnostics tool by clicking **Start > Programs > Citrix > Secure Gateway > Secure Gateway Diagnostics**. This utility contacts all servers running Secure Gateway components and generates a report containing configuration and status information for each component. See "Viewing a Secure Gateway Diagnostics Report" on page 126 for information about using the Secure Gateway Diagnostics tool.

The Secure Gateway event log is another good source of information. To access the event log, click **Start > Programs > Citrix > Secure Gateway > Secure Gateway Management Console**. You may be able to trace the cause of the problem by referring to the error messages in Appendix A.

Scenario B: Double-hop DMZ Deployment

WXYCo, Inc. deployed the Web Interface for access to published resources hosted on computers running MetaFrame Presentation Server. The company plans to deploy the Secure Gateway to provide secure Internet access to published resources.

The security analyst recommended setting up a double-hop DMZ between the Internet and their secure network and securing communications between all Secure Gateway components.



This illustration shows a typical Secure Gateway deployment used to secure a server farm in a double-hop DMZ environment. The secure enterprise network is separated from the Internet by a double-hop DMZ. The enterprise network contains a server farm and a server running the Secure Ticket Authority (STA). The firewall separating the secure network from the second DMZ segment has ports 80, 443, and 1494 open.

If the communications link between the Secure Gateway and the Secure Gateway Proxy is not secured, open port 1080 on the firewall between the first DMZ segment and the second.

The second DMZ segment contains a server running the Secure Gateway Proxy and a second server running the Web Interface. The firewall separating the first and second DMZ segments has port 443 open. The first DMZ segment contains a single server running the Secure Gateway. All traffic originating from the Secure Gateway to servers in the secure network is proxied through the Secure Gateway Proxy.

The Secure Gateway communicates directly with the server running the Web Interface in the second DMZ segment, which in turn communicates directly with servers in the secure network.The first DMZ segment is separated from the Internet by a firewall that has port 443 open.

The mobile workforce carries notebook PCs running a 32-bit Windows operating system, Internet Explorer 5.5, and the MetaFrame Presentation Server Client for 32-bit Windows.

The following sections describe the steps required to deploy the Secure Gateway in this usage scenario.

Printing and Completing the Pre-installation Checklist

Print and complete the *Secure Gateway Pre-installation Checklist*, available from the Documentation Center.

Doing so ensures you complete pre-installation tasks and have configuration information at hand when you are installing Secure Gateway components.

Setting Up and Testing a Server Farm

The steps below are meant to provide a list of tasks you need to complete prior to installing and configuring the Secure Gateway.

1. Install and configure a computer(s) running MetaFrame Presentation Server in the enterprise network.
2. Install, configure, and publish applications on server(s) running MetaFrame Presentation Server.
3. Verify you can launch published applications from a client device.

For detailed instructions about performing these tasks, see the *MetaFrame Presentation Server Administrator's Guide*, available from the Document Center.

Installing and Configuring the STA

The STA issues "session tickets" in response to connection requests for published resources. These session tickets form the basis of authentication and authorization for access to published resources. Per the scenario described, the server running the STA must be located in the secure network.

Important If you are securing communications between the Secure Gateway and the STA, ensure you install a server certificate on the server running the STA.

To install the STA

Before installing the STA, verify the server on which you intend to install the STA meets the installation prerequisites specified in "For the Secure Ticket Authority" on page 41.

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Ticket Authority**. The installation program starts. You must complete the following tasks during installation:
   - Read and accept the license agreement.

- View information specific to the installation of the STA software.
- Ensure that the STA is installed to the same directory as IIS. By default, the STA is installed to \inetpub\scripts\.

Important Ensure you specify the directory to which you installed IIS as the STA installer does not automatically detect the IIS directory.

The files required for STA operation are installed and the Secure Ticket Authority Configuration wizard is launched.

To configure the STA

1. On the **Select configuration level** screen, select **Advanced**.
2. On the **Configure the Secure Ticket Authority** screen, click **Next** to accept default configuration values for the STA.
3. To use the new configuration settings for the STA, you must restart the World Wide Web Publishing Service. If you prefer to restart the service manually, clear the **Restart the Service** check box.
4. Click **Finish** to exit the STA Configuration wizard.

To change configuration parameters for the STA, run the STA Configuration wizard by selecting **Start > Programs > Citrix > Secure Gateway > Secure Ticket Authority Configuration**.

Important Restart the World Wide Web Publishing Service to allow configuration changes to take effect.

Setting Up and Testing the Web Interface

Per the scenario described, you need to set up a Web server running the Web Interface in the second DMZ segment. Ensure you complete the following tasks before you install the Secure Gateway.

1. Install the Web Interface on a stand-alone server in the second DMZ segment.
2. To secure communications between the Secure Gateway and the Web Interface, ensure you install a server certificate on the server running the Web Interface.
3. Add and configure a server farm(s) for use with the Web Interface.
4. Use a Web browser on a client device to connect and log on to the Web Interface.
5. Check that you can launch published applications.

For detailed instructions about performing these tasks, see the *Web Interface Administrator's Guide*, available from the Document Center.

Installing and Configuring the Secure Gateway Proxy

Install the Secure Gateway Proxy on a stand-alone server in the second DMZ segment. If you are securing communications between the Secure Gateway and the Secure Gateway Proxy, ensure you install a server certificate on the server running the Secure Gateway Proxy.

Installing the Secure Gateway Proxy

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Gateway**. The installation wizard is launched and after a brief interval during which the installer checks the server for installed applications, the **Select Components** dialog box appears.
4. In the **Installation mode** section, select **Secure Gateway Proxy**.
5. In the **Citrix MetaFrame products to secure** section, select **MetaFrame XP Servers only**. Click **Next**.
6. Read and accept the license agreement and click **Next**.
7. View the information specific to the component you are installing and click **Next**.
8. Review the information in the **Select Features** dialog box, and click **Next**.
9. Click through the remaining prompts until the installation begins.

When the installation is complete, the configuration wizard is launched.

To configure the Secure Gateway Proxy

1. On the **Select configuration level** screen, select **Advanced**, and select the **Secure traffic between the Secure Gateway Service and the Secure Gateway Proxy** check box.
2. On the **Select a server certificate** screen, select the server certificate to associate with the Secure Gateway Proxy. Click **Next**.
3. On the **Specify secure protocol parameters** screen, click **Next** to accept default values for the **secure protocol** and **cipher suite** that the Secure Gateway Proxy uses to encrypt connections between itself and the Secure Gateway.
4. On the **Configure inbound client connections** screen:
   - Select the **Monitor all IP addresses** check box

- Accept the default value of **443** as the **TCP port** number

This configures the server running the Secure Gateway Proxy to listen for connection requests from the Secure Gateway on all available IP addresses.

5. On the **Configure outbound connections from the Secure Gateway Proxy** screen, select **No outbound traffic restrictions**.
6. On the **Connection parameters** screen, click **Next** to accept default values for connection time-outs and connection limits.
7. On the **Logging Exclusions** screen, click **Add** and enter the IP address(es) of a network device(s), such as load balancers, that you want the Secure Gateway Proxy to exclude from its application log.
8. On the **Logging level** screen, click **Next** to accept the default logging level for the Secure Gateway Proxy.
9. At this point, you completed entry of configuration parameters required for Secure Gateway Proxy operation. The Secure Gateway Proxy must be restarted to reflect changes to its configuration. Select the **Start Secure Gateway Proxy** check box and click **Finish**.

If you need to modify configuration parameters for the Secure Gateway Proxy, run the configuration wizard at a later time by selecting **Start > Programs > Citrix > Secure Gateway > Secure Gateway Service Configuration**.

Installing and Configuring the Secure Gateway

Install the Secure Gateway on a stand-alone server in the first DMZ segment. Ensure a server certificate is installed on this server.

To install the Secure Gateway

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Gateway**. The installation wizard is launched and after a brief interval during which the installer checks the server for installed applications, the **Select Components** dialog box appears.
4. In the **Installation mode** section, select **Secure Gateway Service**.
5. In the **Citrix MetaFrame products to secure** section, select **MetaFrame XP Servers only**. Click **Next**.
6. Read and accept the license agreement and click **Next**.
7. View information specific to the component you are installing and click **Next**.
8. Review information in the **Select Features** dialog box, and click **Next**.
9. Click through remaining prompts until installation begins.

When installation is complete, the Secure Gateway Service Configuration wizard is launched.

To configure the Secure Gateway

1. On the **Select configuration level** screen, select **Advanced**.
2. On the **Select a server certificate** screen, select the server certificate to associate with the Secure Gateway. Click **Next**.
3. On the **Specify secure protocol parameters** screen, click **Next** to accept default values for the **secure protocol** and **cipher suite** that the Secure Gateway uses for client connections.
4. On the **Configure inbound client connections** screen:
   - Select the **Monitor all IP addresses** check box
   - Accept the default value of **443** as the **TCP port** number

   This configures the Secure Gateway to listen for client connection requests on all IP addresses available on this server.
5. Select **Use the Secure Gateway Proxy** as the outbound connection setting. Enter the following details for the Secure Gateway Proxy:

- **FQDN**: Enter the fully qualified domain name of the server running the Secure Gateway Proxy; for example, gwyproxy01.wxyco.com.
- **Secured**: Select this check box to use the default port assignment when connecting to a secure server.

Click **Next**.

6. The **Secure Ticket Authority (STA) details** screen appears. Click **Add**. On the **STA details** screen enter the following information:
   - **FQDN**: Enter the fully qualified domain name of the server running the STA; for example, sta01.wxyco.com.
   - **Path**: Specify the default path and file for the STA. This is typically /Scripts/CtxSTA.dll.
   - **ID**: This field is populated automatically when you click **Next**. The configuration tool contacts the server address you specified. The unique identifier is read from the server running the STA if the configuration wizard successfully resolves the address specified. If the STA cannot be contacted, you are prompted to enter the ID for the STA manually.

     Enter the unique string used to identify the STA. Enter a maximum of 16 alphanumeric characters, uppercase only. Spaces, punctuation, and special characters are not allowed.

   In the **Communication protocol** section, enter the following values:
   - Select the **Secured with HTTPS** check box
   - Select the **Use default** check box to use the default port assignment for connecting to a secure server

   Click **OK**. Click **Next** to proceed with configuration.
7. On the **Connection parameters** screen, click **Next** to accept default values for connection time-outs and connection limits.
8. On the **Logging Exclusions** screen, click **Add** and enter the IP address(es) of a network device(s), such as load balancers, that you want the Secure Gateway to exclude from its application log.
9. On the **Logging level** screen, click **Next** to accept the default logging level for the Secure Gateway.
10. On the **Enter details of the server running Web Interface for MetaFrame XP** screen, do the following:
    - Select **Installed on a different computer** as the **Location**
    - In the **Details** section, enter the FQDN of the server running the Web Interface, for example, webinterface01.xyz.com.
    - Select the **Secured with HTTPS** check box

- In the **TCP Port** box, accept the default value of **443**.

Click **Next**.

11. At this point, you completed the configuration process required for Secure Gateway operation. The Secure Gateway must be restarted to reflect changes to its configuration. Select the **Start Secure Gateway Service** check box and click **Finish**.

If you need to modify configuration parameters for the Secure Gateway, run the configuration wizard at a later time by selecting **Start > Programs > Citrix > Secure Gateway > Secure Gateway Service Configuration**.

Configuring the Web Interface to Support the Secure Gateway

Ensure configuration settings on the server running the Web Interface correctly reflect the details of the STA and the Secure Gateway. For detailed instructions about configuring the Web Interface to support Secure Gateway operation, refer to the *Web Interface Administrator's Guide*, available from the Document Center.

Publishing the URL to Log On to the Secure Gateway

Because all traffic to the Web Interface is proxied through the Secure Gateway, users need to type the following URL to access the logon page:

`https://`*`Secure Gateway FQDN`*`/Citrix/MetaFrame/`

where *Secure Gateway FQDN* is the fully qualified domain name for the server running the Secure Gateway.

In the case of WXYCo, the URL for the logon page is:

`https://www.gateway01.wxyco.com/Citrix/MetaFrame/`

Alternatively, consider changing the default Web root directory in IIS on the server running the Web Interface to point to the Web Interface directory. This enables you to access the logon page by connecting directly to the root URL; that is, https://*Secure Gateway FQDN/*.

In this case, the URL that employees of WXYCo use to access the logon page is:

`https://www.gateway01.wxyco.com/`

Checking Client Devices

Ensure the client devices connecting to the Secure Gateway meet the compatibility requirements stated in "If Your Users Are Connecting to a Server Farm" on page 43.

Testing Your Deployment

After you complete installation and configuration of the Secure Gateway, you need to test that your deployment works and is accessible through the Internet.

1. Use a Web browser on a client device to connect to the server running the Secure Gateway; for example, https://www.gateway01.wxyco.com/citrix/metaframe/.
2. Log on using your domain credentials. After a brief interval, the Applications page containing icons for published applications appears.
3. Verify that you are able to launch published applications from this page.

If you encounter problems loading the logon page, try working your way through the deployment steps to figure out the problem.

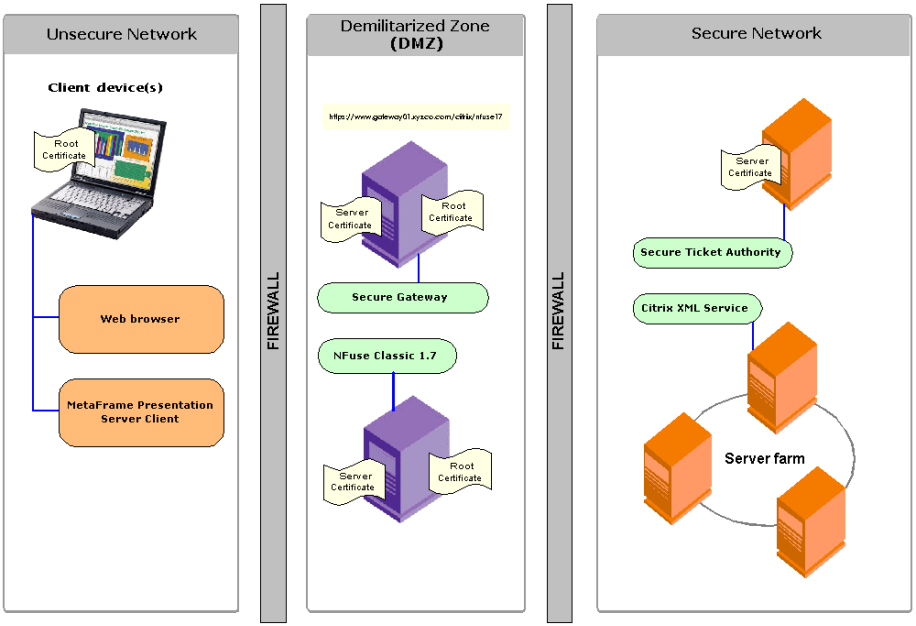
You can run the Secure Gateway Diagnostics tool by clicking **Start > Programs > Citrix > Secure Gateway > Secure Gateway Diagnostics**. This utility contacts all servers running Secure Gateway components and generates a report containing configuration and status information for each component. See “Viewing a Secure Gateway Diagnostics Report” on page 126 for information about using the Secure Gateway Diagnostics tool.

The Secure Gateway event log is another good source of information. To access the event log, click **Start > Programs > Citrix > Secure Gateway > Secure Gateway Management Console**. You may be able to trace the cause of the problem by referring to the error messages in Appendix A.

Scenario C: Upgrading a Secure Gateway, Version 1.x Deployment

XYZCo, Inc. deployed the Citrix Secure Gateway, Version 1.1 to provide secure access to a server farm. Recently, XYZCo purchased to the Citrix MetaFrame Access Suite which includes the Secure Gateway 2.0.

XYZCo’s network administrator recommended to the management that, in addition to upgrading NFuse Classic 1.7 to the Web Interface and MetaFrame XP to MetaFrame Presentation Server, they upgrade the Citrix Secure Gateway, Version 1.1 to the Secure Gateway, Version 2.0.



This diagram illustrates a secure enterprise network separated from the Internet by a single-hop DMZ. The enterprise network contains a server farm and a secure server running the Secure Ticket Authority (STA). The firewall separating the secure network from the DMZ has ports 80, 443, and 1494 open. The DMZ contains a secure server running the Secure Gateway and a second secure server running NFuse Classic, Version 1.7.

At present, users connect directly to the secure server running NFuse Classic, which authenticates the user and redirects authenticated connections to the server running the Secure Gateway. The DMZ is separated from the Internet by a firewall that has port 443 open.

The mobile workforce carries notebook PCs running a 32-bit Windows operating system, Internet Explorer 5.5, and the MetaFrame Presentation Server Client for 32-bit Windows.

The following sections describe the steps required to upgrade an existing deployment of the Citrix Secure Gateway, Version 1.1 to the Secure Gateway, Version 2.0.

Printing and Completing the Pre-installation Checklist

Print and complete the *Secure Gateway Pre-installation Checklist*, available from the Documentation Center.

Doing so ensures you complete pre-installation tasks, and have configuration information at hand when you are installing Secure Gateway components.

Upgrading the Server Farm

Per the scenario described, you need to upgrade your server farm from MetaFrame XP to MetaFrame Presentation Server. For detailed instructions about performing this task, see the *MetaFrame Presentation Server Administrator's Guide*, available from the Document Center.

Upgrading and Configuring the STA

Per the scenario described, you need to upgrade the STA software to Version 2.0. The instructions below guide you through the process of upgrading and configuring the STA.

Important If you are securing communications between the Secure Gateway and the STA, ensure you install a server certificate on the server running the STA.

To upgrade the STA

Before upgrading the STA, verify the server on which you intend to install the STA meets the installation prerequisites specified in "For the Secure Ticket Authority" on page 41.

1. Insert the MetaFrame Presentation Server Components CD.
2. From the Autorun screen, click **Secure Gateway**.
3. Click **Install Secure Ticket Authority**. A message box informs you that an existing version of the software was detected. To upgrade the STA, click **Next**.
4. You must complete the following tasks during installation:
   - Read and accept the license agreement.
   - View information specific to the installation of the STA software.
   - Ensure that the STA is installed to the same directory as IIS. By default, the STA is installed to \inetpub\scripts\.

Important Ensure you specify the directory to which you installed IIS as the STA installer does not automatically detect the IIS directory.

The files required for STA operation are upgraded and the Secure Ticket Authority Configuration wizard is launched.

To configure the STA

1. On the **Select configuration level** screen, select **Advanced**.

2. On the **Configure the Secure Ticket Authority** screen, click **Next** to accept default configuration values for the STA.
3. To use the new configuration settings for the STA, you must restart the World Wide Web Publishing Service. If you prefer to restart the service manually, clear the **Restart the Service** check box.
4. Click **Finish** to exit the STA Configuration wizard.

To change configuration parameters for the STA, run the STA Configuration wizard by selecting **Start > Programs > Citrix > Secure Gateway > Secure Ticket Authority Configuration**.

Important Restart the World Wide Web Publishing Service to allow configuration changes to take effect.

Upgrading and Configuring the Secure Gateway

Per the scenario described, you need to upgrade the Secure Gateway to Version 2.0. The instructions below guide you through upgrading and configuring the Secure Gateway.

To upgrade the Secure Gateway

1. Insert the CD-ROM containing the Secure Gateway software. From the menu displayed, click **Secure Gateway for MetaFrame**. The installation wizard is launched and after a brief interval during which the installer checks the server for installed applications, the **Select Components** dialog box appears.
2. In the **Installation mode** section, select **Secure Gateway Service**.
3. In the **Citrix MetaFrame products to secure** section, select **MetaFrame XP Servers only**. Click **Next**.
4. A message box informs you that an existing version of the software was detected. To upgrade the Secure Gateway, click **Next**.
5. Read and accept the license agreement and click **Next**.
6. View the information specific to the component you are installing and click **Next**.
7. Review information in the **Select Features** dialog box, and click **Next**.
8. Click through remaining prompts until installation begins.

When installation is complete, the Secure Gateway Service Configuration wizard is launched.

To configure the Secure Gateway

1. On the **Select configuration level** screen, select **Advanced**.
2. On the **Select a server certificate** screen, select the server certificate to associate with the Secure Gateway. Click **Next**.
3. On the **Specify secure protocol parameters** screen, click **Next** to accept default values for the **secure protocol** and **cipher suite** that the Secure Gateway uses for client connections.
4. On the **Configure inbound client connections** screen:
   - Select the **Monitor all IP addresses** check box
   - Accept the default port of **443** as the **TCP port** number

   This configures the Secure Gateway to listen for client connection requests on all IP addresses available on this server.
5. On the **Outbound connections from the Secure Gateway Service** check box, select **No Outbound Restrictions**. Click **Next**.
6. The **Secure Ticket Authority (STA) details** screen appears. Click **Add**. On the **STA details** screen enter the following information:
   - **FQDN**: Enter the fully qualified domain name of the server running the STA; for example, sta01.xyzco.com.
   - **Path**: Specify the default path and file for the STA. This is typically /Scripts/CtxSTA.dll.
   - **ID**: This field is populated automatically when you click **Next**. The configuration tool contacts the server address you specified. The unique identifier is read from the server running the STA if the configuration wizard successfully resolves the address specified. If the STA cannot be contacted, you are prompted to enter the ID for the STA manually.

     Enter the unique string used to identify the STA. Enter a maximum of 16 alphanumeric characters, uppercase only. Spaces, punctuation, and special characters are not allowed.

   In the **Communication protocol** section, enter the following values:
   - Select the **Secured with HTTPS** check box
   - Select the **Use default** check box to use the default port assignment for connection to a secure server

   Click **OK**. Click **Next** to proceed with configuration.
7. On the **Connection parameters** screen, click **Next** to accept the default values for connection time-outs and connection limits.

8. On the **Logging Exclusions** screen, click **Add** and enter the IP address(es) of a network device(s), such as load balancers, that you want the Secure Gateway to exclude from its application log.
9. On the **Logging level** screen, click **Next** to accept the default logging level for the Secure Gateway.
10. On the **Enter details of the server running Web Interface for MetaFrame XP**, do the following:
    - Select **Installed on a different computer** as the **Location**
    - In the Details section, enter the FQDN of the server running the Web Interface; for example, WebInterface01.xyz.com
    - Select the **Secured with HTTPS** check box
    - Click **Use default** to use the default TCP port assignment

    Click **Next**.
11. At this point, you completed the entry of configuration parameters required for Secure Gateway operation. The Secure Gateway must be restarted to reflect changes to its configuration. Select the **Start Secure Gateway Service** check box, and click **Finish**.

If you need to modify configuration parameters for the Secure Gateway, run the configuration wizard at a later time by selecting **Start > Programs > Citrix > Secure Gateway > Secure Gateway Service Configuration**.

Upgrading NFuse Classic

Per the scenario described, you need to upgrade the server running NFuse Classic to the Web Interface. In addition, ensure the configuration settings on the server running the Web Interface correctly reflect details of the STA and the Secure Gateway. For detailed instructions about configuring the Web Interface to support Secure Gateway operation, see the *Web Interface Administrator's Guide*, available from the Document Center.

Important If you are securing communications between the Secure Gateway and the Web Interface, ensure you install a server certificate on the server running the Web Interface.

Locking Down IIS

All traffic to the server running the Web Interface is proxied through the server running the Secure Gateway. You need to lockdown IIS to allow only the Secure Gateway to communicate with the Web Interface.

For instructions about configuring IIS to explicitly grant or deny access to applications or Web sites, refer to the IIS documentation that ships with Microsoft Windows Servers.

Publishing the URL to Log On to the Secure Gateway

The URL that users connect to depends on whether you choose to deploy the Web Interface behind or in parallel to the Secure Gateway.

When the Web Interface Is Behind the Secure Gateway

In this scenario, users connect directly to the Secure Gateway. The Web Interface is not accessible through the Internet. All communications to the Web Interface are proxied through the Secure Gateway.

Important Ensure you review the guidance provided in "Web Interface Located Behind the Secure Gateway in the DMZ" on page 88 for information about the advantages and limitations of deploying the Secure Gateway and the Web Interface in this configuration.

Because all traffic to the Web Interface is proxied through the Secure Gateway, users must type the following URL to load the logon page:

```
https://Secure Gateway FQDN/citrix/MetaFrame/
```

where *Secure Gateway FQDN* is the fully qualified domain name for the server running the Secure Gateway. When the Secure Gateway is requested for a connection, it routes the connection request to the server running the Web Interface.

In the case of XYZCo, users must type the URL below to access the logon page:

```
https://www.gateway01.xyzco.com/citrix/MetaFrame/
```

Alternatively, consider changing the default Web root directory in IIS to point to the Web Interface directory. This enables you to access the logon page by connecting directly to the root URL; that is, https://*Secure Gateway FQDN/*.

In this case, the URL employees of XYZCo use to access the logon page is:

```
https://www.gateway01.xyzco.com/
```

To modify the value of the Web root directory in IIS

1. Log on as administrator to the server running the Web Interface.
2. Create a new file called default.asp and save it to the InetPub\wwwroot directory.
3. Edit the default.asp file and add the following line of code:

```
<% Response.Redirect "/citrix/MetaFrame/" %>
```

4. Save and close the file.

When the Web Interface Is Parallel to the Secure Gateway

In this configuration, users connect directly to the server running the Web Interface. In this configuration, the servers running the Secure Gateway and the Web Interface interact exactly as they do in a Citrix Secure Gateway, Version 1.x deployment.

Since users connect directly to the server running the Web Interface, users must type the following URL to load the logon page:

```
https://Web Interface FQDN/citrix/MetaFrame/
```

where, *Web Interface FQDN* is the fully qualified domain name for the server running the Web Interface. In the case of XYZCo, users must type the URL below to access the logon page:

```
https://www.gateway01.xyzco.com/citrix/MetaFrame/
```

Alternatively, consider changing the default Web root directory in IIS to point to the Web Interface directory, as described in "To modify the value of the Web root directory in IIS" on page 113.

Depending on the configuration in which you deployed the Secure Gateway and the Web Interface, inform your users about the URL to enter to access published resources.

Checking Client Devices

Ensure the client devices connecting to the Secure Gateway meet the compatibility requirements stated in "If Your Users Are Connecting to a Server Farm" on page 43.

Testing Your Deployment

After you complete installation and configuration of the Secure Gateway, you need to test that your deployment works and is accessible through the Internet.

1. Use a Web browser on a client device to connect to the server running the Web Interface. The logon page appears.
2. Logon using your domain credentials.
3. After a brief interval, the Applications page containing icons for published applications appears.
4. Check that you are able to launch published applications from this page.

If you encounter problems loading the logon page, try working your way through the deployment steps to figure out the problem.

You can run the Secure Gateway Diagnostics tool by clicking **Start > Programs > Citrix > Secure Gateway > Secure Gateway Diagnostics**. This utility contacts all servers running Secure Gateway components and generates a report containing configuration and status information for each component. See “Viewing a Secure Gateway Diagnostics Report” on page 126 for information about using the Secure Gateway Diagnostics tool.

The Secure Gateway event log is another good source of information. To access the event log, click **Start > Programs > Citrix > Secure Gateway > Secure Gateway Management Console**. You may be able to trace the cause of the problem by referring to the error messages in Appendix A.

Using the Secure Gateway

This chapter describes usage of the management and diagnostic tools available for the Secure Gateway. It also describes the Gateway Client, which is downloaded to client devices from an access center and provides the proxying mechanism required to browse internal Web servers through the Secure Gateway.

This chapter contains the following topics:

- Tools Available When You Install the Secure Gateway
- Using the Configuration Tools
- Using the Secure Gateway Management Console
- Viewing Secure Gateway Performance Statistics
- Using the Gateway Client

Tools Available When You Install the Secure Gateway

When you install the Secure Gateway, shortcuts for the Secure Gateway Service Configuration, the Secure Gateway Management Console, and the Secure Gateway Diagnostics tool are added to the Secure Gateway program menu, which is available when you click **Start > Programs**.

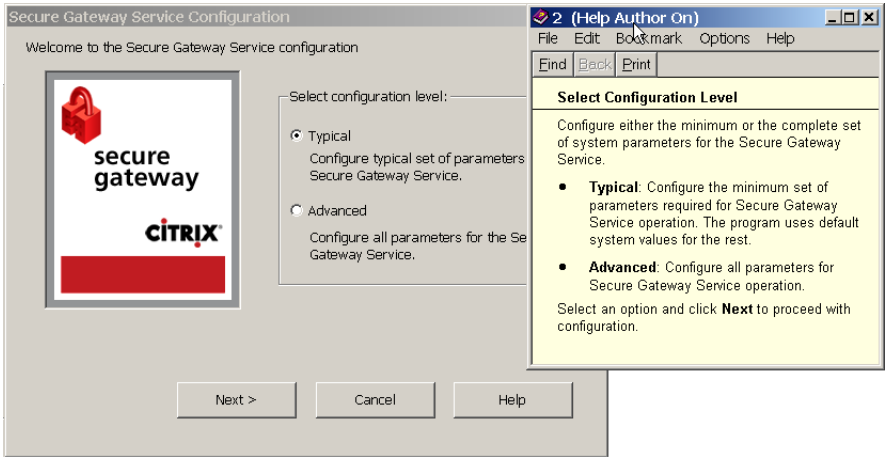
If you install the Logon Agent on the same server as the Secure Gateway, a shortcut to the Logon Agent Configuration wizard is also added to Secure Gateway program menu.



This illustration shows the shortcuts available from the Secure Gateway's program menu.

Using the Configuration Tools

Use the configuration tools to configure Secure Gateway components. To launch the Secure Gateway Service Configuration wizard, click **Start > Programs > Citrix > Secure Gateway > Secure Gateway Service Configuration**.



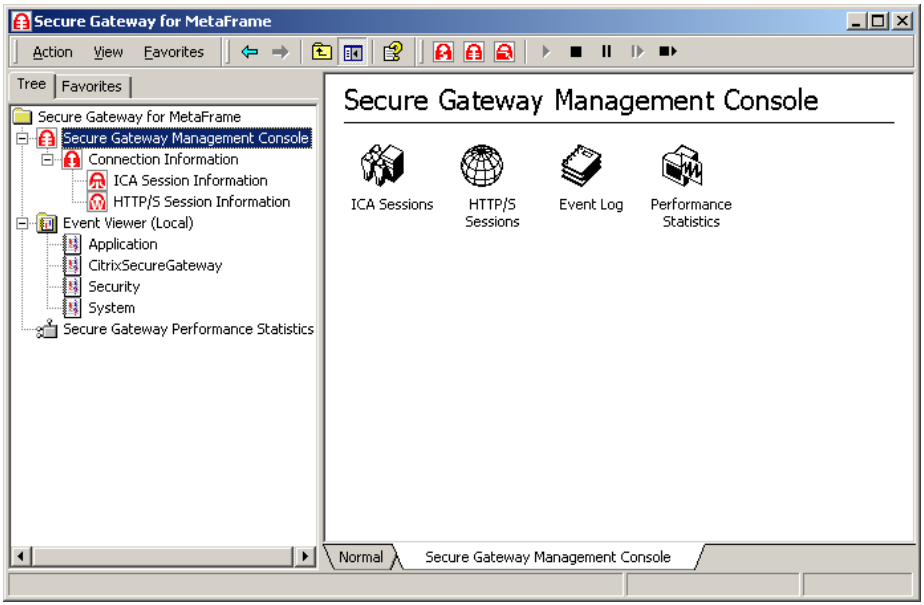
This illustration shows the Secure Gateway Service Configuration wizard and a context-sensitive help screen.

Secure Gateway configuration tools are wizard driven. To access context-sensitive help at any time, click **Help** or press **F1**.

Important If you modify values of parameters such as certificates and STA or Authentication Service details, the Secure Gateway (or the Secure Gateway Proxy) must be restarted for changes to take effect.

Using the Secure Gateway Management Console

The Secure Gateway Management Console is an MMC snap-in and provides an administrator with tools to administer, monitor, and troubleshoot the Secure Gateway.



This illustration shows the Secure Gateway Management Console.

You can start, stop, pause, resume, and restart the Secure Gateway using the icons available on the console toolbar.

In addition, the Secure Gateway Management Console displays the following information:

- All client connections currently running through the Secure Gateway. To refresh the display, right click the **ICA Session Information** node and select **Refresh** or click the **Refresh** icon on the toolbar. To disconnect a client connection, right click on an ICA connection in the right pane and select **Disconnect**.
- All HTTPS connections currently running through the Secure Gateway.

- An instance of the Windows Event Viewer containing contents of the Secure Gateway application log.
- An instance of the Windows Performance Monitor containing performance statistics applicable to the Secure Gateway. Review this list to obtain detailed information regarding the status of client connections running through the Secure Gateway.

The Secure Gateway Management Console also provides access to the following applications:

- Secure Gateway Service Configuration wizard, which allows you to configure operating parameters for the Secure Gateway.
- Secure Gateway Diagnostics tool which presents configuration information and results of communication checks against servers hosting components such as the Logon Agent, STA, Authentication Service, and the Secure Gateway Proxy in the form of a diagnostics report.
- Logon Agent Configuration wizard if the Logon Agent is installed on the same server as the Secure Gateway. If the Logon Agent is installed on a separate server, this icon is disabled.

Viewing Secure Gateway Performance Statistics

Monitoring system performance is an important part of maintaining and administering a Secure Gateway deployment. Performance data can be used to:

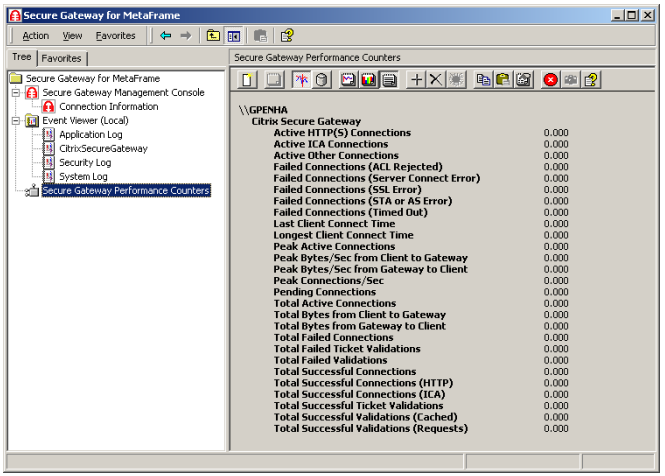
- Understand the workload on the Secure Gateway and the corresponding effect it has on system resources
- Observe changes and trends in workloads and resource usage so you can plan system sizing and failover
- Test changes in configuration or other tuning efforts by monitoring the results
- Diagnose problems and target components or processes for optimization

Citrix recommends that you monitor performance of the Secure Gateway as part of your administrative routine.

You can display an instance of the Windows Performance monitor from the Secure Gateway Management Console.

To view Secure Gateway performance statistics

1. Select **Start > Programs > Citrix > Secure Gateway > Secure Gateway Management Console**.
2. In the tree view, select **Secure Gateway Performance Statistics**. Performance statistics for the Secure Gateway appear in the right pane.



This illustration shows Secure Gateway performance counters.

3. Use the Windows Performance Console controls that appear at the top of the right pane to switch views, add counters, and so on.

Performance Counters Available for the Secure Gateway

The following performance counters are available for the Secure Gateway:

Counter Name	Description
Total Successful Connections (Total)	Specifies the total number of successful client connection requests. This counter is incremented when a client is successfully connected to the requested computer running MetaFrame Presentation Server. It is the sum of total HTTP/S and ICA connections.
Total Successful Connections (HTTP/S)	Specifies the total number of successful HTTP/S client connection requests. This counter is incremented when an HTTP/S client is connected to the requested access center or internal Web server through the Secure Gateway.
Total Successful Connections (ICA)	Specifies the total number of successful ICA connection requests. The counter is incremented when the client is connected to the requested computer running MetaFrame Presentation Server through the Secure Gateway.

Counter Name	Description
Failed Connections (Total)	Specifies the total number of failed client connection requests. The counter is incremented when a client fails to complete the handshaking process or a connection could not be established to the requested resource. It is the sum of the Failed Connections (Timed Out), Failed Connections (SSL Error), Failed Connections (Server Connect Error), Failed Connections (STA or Authentication Service Error), and Failed Connections (ACL Rejected) counters.
Failed Connections (Timed Out)	Specifies the total number of client connection requests that were accepted but timed out before initiating the handshake. The counter is incremented when the client completes the TCP handshake but does not initiate the protocol handshake within the allowed time interval.
Failed Connections (SSL Error)	Specifies the total number of client connection requests that were accepted but did not successfully complete the SSL handshake. The counter is incremented when a client fails to successfully complete the SSL handshake.
Failed Connections (Server Connect Error)	This specifies the total number of client connection requests accepted by the Secure Gateway. These connection requests failed because the Secure Gateway was unable to establish a connection to the requested resource (access center or computer running MetaFrame Presentation Server). The counter is incremented when the Secure Gateway tries to connect to the requested server and cannot. This may occur because the requested server is unavailable or its address cannot be resolved. In a double-hop DMZ deployment, you may get a failed connection error where the Secure Gateway completes connection processing but the Secure Gateway Proxy cannot.
Failed Connections (STA or Authentication Service Error)	Specifies the total number of client connection requests that were accepted but failed due to an unsuccessful validation request to the STA or the Authentication Service. The counter is incremented when the Secure Gateway attempts to validate the ticket or access token with the STA or Authentication Service and validation fails. The validation may fail because the cookie/ticket is invalid/ corrupt, the ticket has expired, or the authority service is unavailable.
Failed Connections (ACL Rejected)	Specifies the total number of client connection requests that failed because the access control lists (ACLs) on the Secure Gateway do not allow the Secure Gateway to establish connections to a requested resource (hosted on an access center or computer running MetaFrame Presentation Server) or to accept connections from a specific client IP address.
Total Bytes from Gateway to Client	Specifies the total number of bytes (for all client connections) sent to the client(s) from the Secure Gateway. The counter is incremented when the Secure Gateway sends data to any connected client.

Counter Name	Description
Total Bytes from Client to Gateway	Specifies the total number of bytes (for all client connections) sent to the Secure Gateway by any connected client. The counter is incremented when the Secure Gateway reads some data from a connected client.
Pending Connections	Specifies the total number of client connection requests that were accepted but have not yet completed the connection process. The connections did not fail or succeed. The counter is incremented when a client connection request is accepted and is decremented when the client connection request succeeds or fails.
Active Connections (Total)	Specifies the total number of client sessions currently active through the Secure Gateway. The counter is incremented for each successful client connection request and is decremented for each disconnected or terminated connection. Active Connections (Total) is the sum of the values of Active Connections (ICA), Active Connections (HTTP/S), and Active Connections (Other) counters.
Active Connections (ICA)	Specifies the total number of ICA sessions currently active through the Secure Gateway. The counter is incremented for each successful ICA connection request and decremented for each disconnected or terminated ICA connection.
Active Connections (HTTP/S)	Specifies the total number of HTTP/S client sessions currently active through Secure Gateway. It is incremented for each successful client connection request and is decremented for each disconnected or terminated HTTP/S connection.
Active Connections (Other)	These are the connections to the Logon Agent or the Web Interface to a computer running MetaFrame Presentation Server. Specifies the total number of client sessions currently active through the Secure Gateway that are not yet authenticated. The counter is incremented for each successful client connection request and is decremented for each disconnected or terminated non-ICA or HTTP/S connection.
Peak Active Connections	Specifies the maximum number of concurrent connections that were established through the Secure Gateway since the Secure Gateway was last started. The counter is updated every time the value of Active Connections (Total) exceeds the current Peak Active Connections counter.
Peak Bytes/Sec from Gateway to Clients	Specifies the maximum data throughput rate from the Secure Gateway to clients.
Peak Bytes/Sec from Client to Gateway	Specifies the maximum data throughput rate from clients to the Secure Gateway.
Peak Successful Connections/Sec	Specifies the maximum number of successful client connection requests per second since the Secure Gateway was started.

Counter Name	Description
Last Client Connect Time	Specifies the time taken by the last successful client connection request to complete the connection process. The counter is updated when a client connection request completes successfully.
Longest Client Connect Time	Specifies the longest time taken for a client connection request to complete successfully. The value of this counter is checked when a client connection request completes successfully. The counter is updated if the last client connection request that successfully completed took longer to complete than the current value of Longest Client Connect Time.
Total Successful Ticket Validations	This counter provides STA-related information. The Secure Gateway connects to the STA and requests ticket validation. The counter is updated when the STA validates the ticket and returns the information stored in its cache for the ticket. The update occurs during the handshake process before the Secure Gateway attempts to connect to the requested computer running MetaFrame Presentation Server.
Total Failed Ticket Validations	Specifies the total number of unsuccessful STA ticket validation requests. If a ticket is not validated by the STA or the Secure Gateway, this counter is incremented.
Total Successful Validations (Requests)	Specifies the total number of successful validations by the Authentication Service in response to access token validation requests from the Secure Gateway. When the Secure Gateway fails to validate an access token against the contents of its cache, it requests the Authentication Service to validate the access token. The counter is incremented when the Authentication Service returns a validation successful message.
Total Successful Validations (Cached)	Specifies the total number of successful access token validations in the case when the Secure Gateway is able to validate an access token against the contents of its cache. The counter is incremented when the Secure Gateway successfully validates an access token by checking if it has the access token in its cache.
Total Failed Validations	This is the total number of unsuccessful access token validations. This counter is incremented if an access token cannot be validated by the Authentication Service or there is an error while the Secure Gateway is attempting to validate the access token.

Viewing Secure Ticket Authority Statistics

In addition to monitoring the performance of the server running the Secure Gateway, Citrix recommends monitoring the performance of the server running the STA as part of your administrative routine.

To view STA performance statistics

1. Access the Performance Monitor.

2. Right click in the right pane and click **Add Counters**.
3. For the location of the performance counters, select **Use local computer counters**.
4. Select **Secure Ticket Authority** from the **Performance Object** drop-down list.
5. Select the performance counters you want to monitor and click **Add**.
6. Click **Close**.
7. Use the Windows Performance Console controls that appear at the top of the right pane to switch views, add counters, and so on.

Performance Counters Available for the STA

The following performance counters are available for the Secure Ticket Authority:

Performance Counter	Description
STA Bad Data Request Count	The total number of unsuccessful ticket validation and data retrieval requests during the lifetime of the STA.
STA Good Data Request Count	The total number of successful ticket validation and data retrieval requests received during the lifetime of the STA.
STA Bad Ticket Request Count	The total number of unsuccessful ticket generation requests received during the lifetime of the STA.
STA Good Ticket Request Count	The total number of successful ticket generation requests received during the lifetime of the STA.
STA Peak Data Request Rate	The maximum rate of data requests per second during the lifetime of the STA.
STA Peak Ticket Request Rate	The maximum rate of ticket generation requests per second during the lifetime of the STA.
STA Peak All Request Rate	The maximum rate of all monitored activities per second.
STA Ticket Timeout Count	The total number of ticket time-outs that occur during the lifetime of the STA.
STA Count of Active Tickets	Total count of active tickets currently held in the STA.

Viewing a Secure Gateway Diagnostics Report

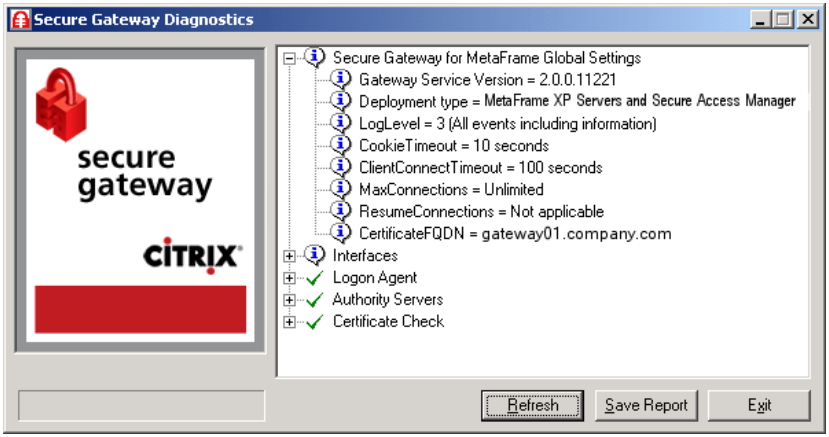
The Secure Gateway Diagnostics tool presents configuration information and results of communication checks against servers hosting components such as the Logon Agent, STA, Authentication Service, and the Secure Gateway Proxy in the form of a diagnostic report. It's a quick and easy way of performing a series of checks to ascertain the health and status of Secure Gateway components.

To run Secure Gateway Diagnostics

To launch the Secure Gateway Diagnostics tool, select **Start > Programs > Citrix > Secure Gateway > Secure Gateway Diagnostics**.

–or–

Start the Secure Gateway Management Console and click the Secure Gateway Diagnostics icon. The Secure Gateway Diagnostics window appears.



This illustration shows a Secure Gateway Diagnostic report.

The Diagnostics tool scans the registry and reports global settings for the Secure Gateway. It uses the Secure Gateway configuration information to contact servers running the Logon Agent, the Secure Gateway Proxy, the STA, and the Authentication Service, if used, and reports whether or not the communication check passed or failed. It examines the server certificate installed on the server running the Secure Gateway and checks credentials and validity.

In the Secure Gateway Diagnostics window, information icons indicate that a registry or configuration value is present:

Information icon	A registry or configuration value is present
Warning icon	A registry or configuration value is missing
Passed check icon	A communication check for the component passed
Failed check icon	A communication check for the component failed

For any component marked with a warning or failed check icon, verify that you properly installed the component and provided all necessary configuration information.

The information available in a typical Secure Gateway Diagnostics report is described in the following sections.

Global Settings

Configuration settings for the Secure Gateway are stored in the Windows registry. The Secure Gateway Diagnostics tool scans the registry and returns the following values:

```
Secure Gateway Diagnostics Version 2.0.0.11337

Computer NetBIOS Name: GATEWAY01
Configuration captured on: 2/27/2003 9:44:55 AM
-----------------------------------------------

Secure Gateway for MetaFrame Global Settings
-------------------------------------------
  Gateway Service Version = 2.0.0.11337
  Deployment type = MetaFrame XP Server and Secure Access Manager
  LogLevel = 3 (All events including information)
  CookieTimeout = 10 seconds
  ClientConnectTimeout = 100 seconds
  MaxConnections = Unlimited
  ResumeConnections = Not applicable
  CertificateFQDN = gateway01.company.com
```

Interfaces

This section contains values for one or more IP interface and port combinations that the Secure Gateway is configured to use.

```
Interfaces
----------

  All interfaces (0.0.0.0 : 443)
  ------------------------------
    Protocol = BOTH
    Ciphers = ALL
    Secured = Yes
    HTTP = Yes
    ICA = Yes
    SOCKS = No
    Gateway Client = Yes
    LoadBalancerIPs = 17.34.124.233
```

Secure Gateway Proxy

This section contains information about the Secure Gateway Proxy, if used, and whether or not the Secure Gateway was able to establish a connection to it.

```
Secure Gateway Proxy - All output is directed to a Secure Gateway Proxy
-----------------------------------------------------------------------
  FQDN = gwyproxy.company.com
  Port = 1080
  Secured = No
  Protocol = BOTH
  Ciphers = ALL
  Tested OK
```

Logon Agent

This section contains information about the Logon Agent and whether or not the Secure Gateway was able to establish a connection to it.

```
Logon Agent
-----------
  FQDN = localhost
  Port = 80
  Secured = No
  Protocol = BOTH
  Ciphers = ALL
  Tested OK
```

Authority Servers

The STA and the Authentication Service are collectively referred to as *authority servers*. This section contains information about the servers running the Authentication Service and/or the STA, and whether or not the Secure Gateway was able to establish a connection to these components.

```
Authority Servers
-----------------

  ID = ccT5447UTkNcKmr4
  ---------------------
    FQDN = as01.company.com
    Server = as01.company.com
    Port = 443
    Path = /access_center01/AuthService/AuthService.asmx
    Type = AS
    Secured = Yes
    Protocol = BOTH
    Ciphers = ALL
    Tested OK

  ID = STAFE565EE5A52E
  --------------------
    FQDN = sta01.company.com
    Server = sta01.company.com
    Port = 443
    Path = /Scripts/CtxSTA.dll
    Type = STA
    Secured = Yes
    Protocol = BOTH
    Ciphers = ALL
    Tested OK
```

Certificate Check

This section contains information about the server certificate installed on the server running the Secure Gateway and whether it is valid for the current system date.

```
Certificate Check
-----------------
  FQDN = gateway01.company.com
  This certificate is currently valid.
  No information status reported.
```

Using the Gateway Client

Web servers aggregated through an access center can be Web servers that host access centers, Web servers that host other Intranet Web sites (referred to as *internal Web servers*), or both.

The Gateway Client is an ActiveX control that downloads and installs automatically to an authenticated remote client browser. When installed, it provides the proxying mechanism required to access internal Web servers aggregated through an access center.

The Gateway Client functions in a manner similar to a VPN. It enables client Web browsers to access internal Web sites that are available from an access center. All content and resources available on internal Web sites or servers are protected by the Gateway Client using SSL or TLS.

The Gateway Client inspects all data originating from the client Web browser and directs all requests for resources available in the access center or an internal Web server, to the Secure Gateway. If the client browser requests access to an external Web site, the Gateway Client resolves the browser request as an external Web site, for example, http://www.cnn.com/.

The Gateway Client traverses client-side proxy servers, if any, to reach the destination server, that is the Secure Gateway or an external Web site.

Warning Be aware that there are some risks involved in allowing an internal Web site to be accessed through the Internet. Administrators must ensure that internal Web sites are secured before exposing them to the Internet. There are also risks to users when accessing Web sites on the Internet. By default, the Secure Gateway is placed in the Internet zone, internal Web sites are normally placed into the Local intranet zone by the Web browser. The Gateway Client restricts internal Web sites to the same security level as the server running the Secure Gateway. Users can grant greater security privileges to internal Web sites by adding the URL of the Secure Gateway into a more trusted zone. Ensure users are aware of the risks in doing this and trust the site they are accessing. Citrix recommends that you provide instructions for configuring security zones in Internet Explorer on the client device to users of the Gateway Client. For detailed information about security zones in Internet Explorer see the Microsoft Knowledge Base Article 174360, "How to Use Security Zones in Internet Explorer".

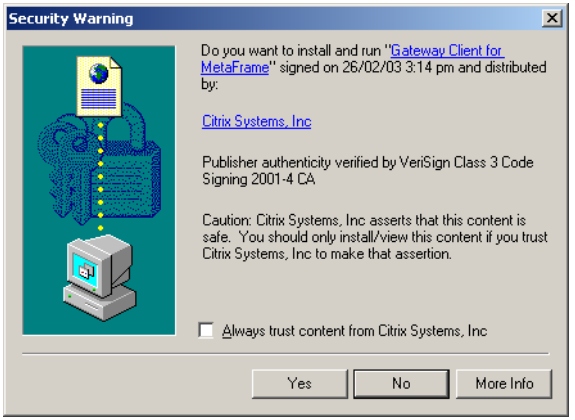
Downloading the Gateway Client

The Gateway Client must be installed on the client devices of users accessing an access center through the Secure Gateway.

1. When you log on to an access center through the Secure Gateway, a security warning prompting you to install and run the Gateway Client appears. The Gateway Client enables users to access internal Web sites that are aggregated through the access center.

   By agreeing to download and install the Gateway Client, you agree to trust the ActiveX control signed by Citrix Systems, Inc.

Important Citrix recommends that you ensure the Gateway Client is a genuine copy signed by Citrix Systems, Inc. before you agree to download it. Click **More Info** in the **Security Warning** dialog box for details. If in doubt about its authenticity, click **No**. For instructions about using the Gateway Client, see "Using the Gateway Client" on page 130.



*This illustration shows the **Security Warning** dialog box associated with the Gateway Client.*

2. Click **Yes** to proceed with download and installation of the Gateway Client.

   The Gateway Client installs into the client Web browser's Downloaded Program Files folder, typically located in the %systemroot%\Downloaded Program Files directory.

3. When download and installation of the Gateway Client is complete, you can browse or access internal Web servers available from the access center.

Note Updated versions of the Gateway Client, if available, are automatically downloaded to the client device once logged on.

How to Use the Gateway Client

When you log on to an access center, the Gateway Client, if present on the client device, is invoked.

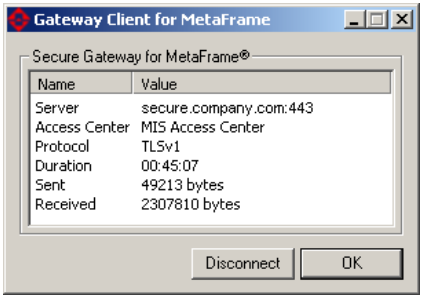
All Internet Explorer browser windows proxied through the Secure Gateway contain the Gateway Client icon in the top left corner of the status bar.



This illustration shows a typical access center page populated with Web pages, published resources, and alert messages.

Important The Gateway Client is not automatically invoked when you spawn new instances of Internet Explorer by clicking its desktop icon or Start menu shortcut. To use the Gateway Client in more than one Web browser window, launch new instances of Internet Explorer by selecting **File > New > Window** in the Web browser window that is already running the Gateway Client.

When connected to the access center, a Gateway Client icon appears in the system notification tray (systray). Click the systray icon to display the Gateway Client status window.



This illustration shows the Gateway Client status window.

To disconnect from an access center, click **Disconnect**. All browser connections currently proxied through the Gateway Client are terminated.

Optimization and Security Guidelines

This chapter provides general compatibility guidelines for deploying the Secure Gateway in complex network environments containing components such as load balancers, SSL accelerator cards, firewalls, and so on. This chapter contains the following topics:

- Configuring Firewalls
- Planning for High Availability
- Load Balancing a Secure Gateway Server Array
- Recommendations for Improving Security

Configuring Firewalls to Handle ICA Traffic

A firewall is a device designed to stop unauthorized access to a network. It may also protect the network from certain kinds of disruptions, network viruses, and so on. Firewalls are positioned between a network and the Internet, so that all network traffic between these flows through the firewall.

The Secure Gateway for is designed to facilitate secure Internet access to applications and resources hosted on server farms in a secure, enterprise network. The Secure Gateway is typically deployed in the DMZ, a network segment that creates a secure perimeter between the Internet and the secure network. This usually means that traffic originating from a remote client device must traverse firewalls to get to the destination server in the secure network. It is, therefore, crucial to Secure Gateway operation that firewalls are configured to allow HTTPS and ICA/SSL traffic traversal. Correct firewall configuration can help prevent disconnects and contribute toward better performance of the Secure Gateway.

Of particular concern with regard to firewall traversal is ICA/SSL traffic which is a Citrix-proprietary protocol used for communications between client devices and computers running MetaFrame Presentation Server. Firewalls are not ICA aware and do not make any distinction between HTTPS or ICA/SSL traffic. The ICA protocol is a real-time, interactive protocol that is very sensitive to latency and other network delays. Because ICA traffic typically consists of mouse-clicks and keystrokes, delays in their transmission could result in significantly degraded performance of the connection. In contrast, HTTPS traffic is less sensitive to latency or other types of network delays. Therefore, HTTPS connections to computers running MetaFrame Presentation Server are less affected than ICA connections to computers running MetaFrame Presentation Server.

To ensure that users experience usable and reliable sessions when using the Secure Gateway, Citrix recommends configuring your firewall to work in forwarding mode as opposed to proxy mode. Set the firewall to use its maximum inspection level. Configuring your firewall to use forwarding mode ensures that TCP connections are opened directly between remote client devices and the Secure Gateway.

However, if you prefer to configure your firewall to use proxy mode, ensure that your firewall does not:

- Impose any time-outs on ICA/SSL sessions, including idle, absolute, and data traffic time-outs
- Use the Nagle algorithm for ICA/SSL traffic
- Impose any other specific restrictions or filters on ICA/SSL traffic

It is important to note that if you use a firewall that is ICA aware, the issues outlined above may not apply.

Planning for High Availability

You can design your Secure Gateway deployment to ensure high availability by deploying multiple servers running the Secure Gateway.

Deploying multiple servers running the Secure Gateway does not make an ICA or HTTP/S session fault tolerant, but provides an alternative server if one server fails.

When the number of concurrent ICA or HTTPS sessions exceeds the capacity of a single server running the Secure Gateway, multiple servers running the Secure Gateway must be deployed to support the load. There is no practical limit to the number of servers running the Secure Gateway that can be deployed to service large access centers or server farms.

To deploy multiple servers running the Secure Gateway, a load balancer is required. The function of the load balancer is to distribute client sessions to one of a number of servers offering a service. This is normally done by implementing a *virtual address* on the load balancer for a particular service and maintaining a list of servers offering the service. When a client connects to a service, the load balancer uses one of a number of algorithms to select a server from the list and directs the client to the selected server.

The algorithm can be as simple as a “round robin” where each client connect request is assigned to the next server in a circular list of servers, or a more elaborate algorithm based on machine load and response times.

The client response to a server failure depends on which server fails and at what point in the session the server fails.

- The server running the Web Interface is involved during user sign on, application launch, or application relaunch. Failure of the Web Interface requires you to reconnect to the logon page and sign on again when you want to launch a new application or relaunch an existing application.
- The STA is involved in the launch or relaunch of an application. Failure of the STA during application launch requires that you return to the published applications page on the access center or the Web Interface to relaunch the application.
- The Secure Gateway is involved during application launch, and the time an application remains active. Failure of the Secure Gateway requires that you return to the logon page to repeat the authentication process.

Intelligent load balancers can also detect the failure of a server through server polling, temporarily remove the failed server from their list of available servers, and restore them to the list when they come back online.

Load Balancing an Array Secure Gateways

A load balancing solution managing an array of servers running the Secure Gateway can provide the following key benefits, including:

Scalability. Performance of a Secure Gateway implementation is optimized by distributing its client requests across multiple servers within the array. As traffic increases, additional servers are added to the array. The only restriction to the maximum number of servers running the Secure Gateway in such an array is imposed by the load balancing solution in use.

High availability. Load balancing provides high availability by automatically detecting the failure of a server running the Secure Gateway and redistributing client traffic among the remaining servers within a matter of seconds.

Load balancing an array of servers running the Secure Gateway is accomplished using a virtual IP address that is dynamically mapped to one of the real IP addresses (for example, 10.4.13.10, 10.4.13.11, and 10.4.13.12) of a server running the Secure Gateway. If you use a virtual IP address such as 10.4.13.15, all your requests are directed to the virtual IP address and then routed to one of the servers. You can set up the virtual IP address through software, such as Windows NT Load Balancing Service (WLBS), or hardware solutions, such as a Cisco CSS 11000 Series Content Services switch. If you use hardware in a production environment, make sure you use two such devices to avoid a single point of failure.

Load Balancing an Array of Secure Gateway Proxies

You can load balance an array of servers running the Secure Gateway Proxy in the same way as the Secure Gateway.

This is useful in situations where you experience extremely high loads on the Secure Gateway array, in which case, it may help to deploy a second Secure Gateway Proxy and load-balance the two servers.

In addition, if the communications link between the Secure Gateway and the Secure Gateway Proxy is secured, you can use a single certificate for the Secure Gateway Proxy array.

Certificate Requirements

Load balancing relies on the use of a virtual IP (VIP) address. The VIP address is bound to an FQDN and all clients request connections from the VIP address rather than the individual servers running the Secure Gateway behind it. Basically, a single IP address, the VIP, acts as an entry point to your servers running the Secure Gateway, simplifying the way clients access Web content, published applications, and services on computers running MetaFrame Presentation Server.

If you are using a load balancing solution, all servers running the Secure Gateway can be accessed using a common FQDN; for example, csgwy.company.com.

In conclusion, you need a single server certificate, issued to the FQDN (mapped to the virtual IP or DNS name) of the load balancing server. The certificate must be installed on every server running the Secure Gateway in the server array that's being load balanced.

Load Balancers and SSL Accelerator Cards

Load balancing solutions available in the market today may feature built-in SSL accelerator cards. If you are using such a solution to load balance an array of servers running the Secure Gateway, disable the SSL acceleration for traffic directed at the servers running the Secure Gateway. Consult the load balancer documentation for details about how to do this.

Presence of SSL accelerator cards in the network path before the server running the Secure Gateway means the data arriving at the Secure Gateway is decrypted data. This conflicts with a basic function of the Secure Gateway, which is to decrypt SSL data before sending it to a computer running MetaFrame Presentation Server. The Secure Gateway does not expect non–SSL traffic and drops the connection.

Using Multiple STAs

You do not need an external load balancing device to deploy multiple servers running the STA. Citrix provides a mechanism for defining multiple STAs as described below.

Due to the small processing load involved in issuing a ticket and returning ticket details, a single server running the STA is capable of supporting a very large number of users. Two servers running the STA can be configured for redundancy purposes.

When using multiple servers running the STA, ensure each STA is assigned a unique identifier, such as STA01, STA02, and so on. If more than one server running the Web Interface is used, you can configure each server with a different STA entry at the head of its configured list of STAs. This ensures the ticketing load is distributed across the available STAs.

Keep–Alive Values and MetaFrame Presentation Server

If you enabled TCP/IP keep–alive parameters on computers running MetaFrame Presentation Server, Citrix recommends that you modify the parameters on the server running the Secure Gateway in the same manner.

This is required because in an environment containing the Secure Gateway, ICA and HTTP/S connections are routed through the Secure Gateway. TCP/IP keep–alive messages from the computer running MetaFrame Presentation Server to the remote client are intercepted and responded to by the server running the Secure Gateway. Similarly TCP/IP keep–alive packets from the server running the Secure Gateway are sent only to the client device; the server running the Secure Gateway does not transmit keep–alives to the computer running MetaFrame Presentation Server or the STA. Setting the keep–alive values on the server running the Secure Gateway to match the values set on the computer running MetaFrame Presentation Server ensures that the server farm is aware of the client connection state and can either disconnect or log off from the connection in a timely manner.

See the Citrix Knowledgebase Article CTX708444 – "How to Configure TCP and ICA KeepAlive Values So TCP/IP Users Go to Disconnected State" for more information about the use of ICA and TCP/IP keep–alives on computers running MetaFrame Presentation Server.

Connection Keep–Alive Values and the Secure Gateway

The Secure Gateway establishes connections over the Internet between remote clients and computers running MetaFrame Presentation Server. When a client connection is dropped without being properly logged off, the Secure Gateway continues to keep the connection to the computer running MetaFrame Presentation Server open. Accumulation of such "ghost" connections eventually affects the Secure Gateway's performance.

A Secure Gateway deployment subject to heavy load may run out of sockets because of these "ghost" connections remaining open. The Secure Gateway uses TCP/IP keep-alives to detect and close broken connections between the Secure Gateway and the client device. The default Windows setting for KeepAliveTime is 7,200,000 milliseconds or two hours. This is the duration that TCP/IP waits before verifying whether an idle connection is still connected.

If there is no response, TCP/IP retries the verification process after the interval specified by KeepAliveInterval and for a maximum number of times specified by TcpMaxDataRetransmissions. The default value for KeepAliveInterval is one second, and the default value for TcpMaxDataRetransmissions is five.

This means that "ghost" connections may remain open for up to two hours (7,200,000 milliseconds) before the system detects that a connection failed. If this is a problem, Citrix recommends that you reduce KeepAliveTime to a value more suitable to your network usage profile. You may need to modify keep-alive parameters or disable them depending on your network environment.

If the Secure Gateway is under heavy load and is used predominately to secure HTTP connections to MetaFrame Secure Access Manager or internal Web servers, the Secure Gateway rapidly opens and closes connections. Closed connections stay in the TIME_WAIT state for an interval specified by TcpTimedWaitDelay.

The default value of TcpTimedWaitDelay is 4 minutes (240 seconds); the Secure Gateway sets this value to thirty seconds. This change enables the Secure Gateway to recycle sockets faster resulting in improved performance. The system cannot reuse sockets in the TIME_WAIT state. MaxUserPort specifies the number of sockets available on the system. By default, the system uses ports between 1024 and 5000; the Secure Gateway modifies this setting to use ports between 1024 and 65000.

The KeepAliveInterval, KeepAliveTime, MaxUserPort, TcpMaxDataRetransmissions, and TcpTimedWaitDelay parameters are stored in the Windows registry:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\

Consult Microsoft Knowledgebase articles, Q120642 - “TCP/IP & NBT Configuration Parameters for Windows 2000 or Windows NT,” Q314053 - “TCP/IP & NBT Configuration Parameters for Windows XP,” and Q196271 - “Unable to Connect from TCP Ports Above 5000” for information about making changes to these parameters. Under normal circumstances, it is not necessary to change these settings.

Warning Using the Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee resolution of problems resulting from the incorrect use of Registry Editor. Use Registry Editor at your own risk.

Recommendations for Improving Security

The Secure Gateway is an application–specific proxy designed to achieve a corresponding level of security. It is not a firewall and should not be used as such. Citrix recommends that you use a firewall to protect servers running the Secure Gateway, MetaFrame Presentation Server, and other corporate resources from unauthorized access from the Internet and internal users.

Deploying the Secure Gateway in the DMZ

Place the Secure Gateway in the DMZ between two firewalls for maximum protection. In addition, physically secure the DMZ to prevent access to the firewalls and servers within the DMZ. A breach of your DMZ servers may, at best, create an annoyance in the form of downtime while you recover from the security breach.

Warning Citrix recommends that you configure your firewalls to restrict access to specific TCP ports only. If you configure your firewalls to allow access to TCP ports other than those used for HTTP, ICA, SSL, and XML data, you may allow users to gain access to unauthorized ports on the server.

Restricting Ciphersuites

The process of establishing a secure connection involves negotiating the ciphersuite that is used during communications. A ciphersuite defines the type of encryption that's used—it defines the cipher algorithm and its parameters, such as the size of the keys.

Negotiation of the ciphersuite involves the client device informing the Secure Gateway which ciphersuites it is capable of handling, and the Secure Gateway informing the client which ciphersuite to use for client-server communications.

The Secure Gateway supports two main categories of ciphersuite: COM (commercial) and GOV (government). The ALL option includes both the commercial and government suites.

The COM ciphersuites are:

- SSL_RSA_WITH_RC4_128_MD5 or {0x00,0x04}
- SSL_RSA_WITH_RC4_128_SHA or {0x00,0x05}

The GOV ciphersuite is:

- SSL_RSA_WITH_3DES_EDE_CBC_SHA or {0x00,0x0A}

Some organizations, including U.S. government organizations, require the use of government-approved cryptography to protect sensitive but unclassified data.

To restrict the ciphersuites available

1. Log on as an administrator to the server running the Secure Gateway.
2. Click **Start > Programs > Citrix > Secure Gateway > Secure Gateway Service Configuration**.
3. Select **Advanced** configuration and click **Next** until you see the **Configure secure protocol parameters** screen.

   The default setting for ciphersuites is ALL. To restrict the ciphersuite, change the value to **GOV** or **COM**, as required. Click **Next**.
4. Follow prompts until configuration is complete. Click **Finish** to exit the configuration wizard.

Important You must restart the Secure Gateway to let configuration changes take effect.

Restricting Ciphersuites Used for Communications between the Secure Gateway and the Secure Gateway Proxy

The ciphersuites used to secure communications between the Secure Gateway and the Secure Gateway Proxy are determined by the configuration settings on the server running the Secure Gateway Proxy. The default setting on the Secure Gateway for outgoing connections to the Secure Gateway Proxy is set to use all ciphersuites.

Security policies of some organization may require tighter control of the ciphersuites offered by the Secure Gateway for outgoing connections to the Secure Gateway Proxy. This can be achieved by modifying SChannel registry settings.

For instructions about modifying SChannel registry settings to restrict ciphersuites, refer to the Microsoft Knowledge Base Article Q245030, “How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll.”

Using Secure Protocols

The Secure Gateway is designed to handle both SSL Version 3 and TLS Version 1 protocols. It is important to note the following in this context:

- The Gateway Client is set to use TLS Version 1 as the default
- Internet Explorer is set to use SSL Version 2 and 3 as the default.

You can restrict the Secure Gateway to accept only SSL Version 3 or TLS Version 1 connections. If you decide to change the default protocol setting on the Secure Gateway, ensure you modify protocol settings on the client Web browser as well as the Gateway Client to match the protocol setting on the server running the Secure Gateway.

As a general rule, Citrix recommends against changing the default setting for the secure protocol used by the Secure Gateway.

Removing Unnecessary User Accounts

Citrix recommends removing all unnecessary user accounts on servers running Secure Gateway components.

Avoid creating multiple user accounts on servers running Secure Gateway components, and limit the file access privileges granted to each account. Review active user accounts regularly and when personnel leave.

Removing Sample Code Installed with IIS

An important security step is to disable or remove all the IIS-installed sample Web applications. Never install sample sites on production servers because of the many well-identified security risks they present. Some sample Web applications are installed so that you can access them only from http://localhost or the IP address 127.0.0.1. Nevertheless, you should remove the sample sites. The IISSamples, IISHelp, and Data Access virtual directories and their associated folders are good examples of sample sites that should not reside on production servers.

Secure Components that Run on IIS

The STA and the Logon Agent are hosted by IIS, and are therefore vulnerable to any security flaws inherent to IIS. To ensure that security of Secure Gateway components is not compromised, you can do the following:

Set appropriate ACLs on IIS. The Logon Agent and the STA are hosted by IIS. To prevent unauthorized access to executables and script files, Citrix recommends setting appropriate ACLs on IIS. For instructions about locking down IIS, refer to current Microsoft product documentation and online resources available from the Microsoft Web site.

Secure all Secure Gateway components using SSL or TLS. This ensures that data communications between all Secure Gateway components is encrypted. For instructions about securing Secure Gateway components, see previous chapters in this guide.

To maximize the security of the servers running Secure Gateway components hosted by IIS, follow Microsoft security guidelines for locking down Internet Information Services on Windows Servers.

Stopping and Disabling Unused Services

All Windows services introduce a level of vulnerability, so it is important to disable the services that are not required.

To disable a Windows service

1. Right-click **My Computer** and select **Manage**.
2. In the Computer Management Console, select **Services**.
3. Highlight the service you want to disable and select **Properties**.
4. In the service Properties dialog box, select **Disabled** as the **Startup Type**.

Repeat the process for each service you want to disable.

Installing Service Packs and Hotfixes

Ensure that you install all operating system-specific service packs and hotfixes, including those applicable to applications and services that you are running on the system.

Ensure you do not install hotfixes for services that are not installed. Ensure you regularly review Security Bulletins from Microsoft. These are available online at http://www.microsoft.com/technet/security/current.asp.

Following Microsoft Security Guidelines

Citrix recommends that you review Microsoft guidelines for securing Windows servers. These guidelines are available at http://www.microsoft.com/technet/security/prodtech/windows/secwin2k/default.asp.

In general, refer to the Microsoft Web site for current guidance to help you understand and implement the processes and decisions that must be made to get, and stay, secure.

Troubleshooting

The Secure Gateway must be configured correctly to prevent connection errors or failures. This section provides basic techniques to assist you in troubleshooting potential problems that could occur with a Secure Gateway deployment.

This chapter contains the following topics:

- General Troubleshooting Procedures
- Common Problems
- If You Are Still Unable to Resolve the Problem

General Troubleshooting Procedures

This section contains general guidelines and advice for troubleshooting a Secure Gateway deployment.

Assumptions

It is assumed that you installed and configured the Secure Gateway as described in preceding chapters of this guide.

Note Troubleshooting information concerning firewall traversal, Domain Name Service (DNS), and Network Address Translation (NAT) are beyond the scope of this document.This chapter assumes that you correctly configured NAT and packet filtering on your network.

Checking Results Reported by Secure Gateway Diagnostics

The Secure Gateway Diagnostics tool is designed to perform a quick check to determine that the Secure Gateway is configured correctly and that it is able to resolve addresses and communicate with servers located in the DMZ and the secure network.

Run the Secure Gateway Diagnostics tool on the server running the Secure Gateway and examine the results reported. The report contains configuration values for the Secure Gateway and results of connection attempts to components and services in the DMZ and secure network that the Secure Gateway uses.

The results reported by the Secure Gateway Diagnostics tool are sufficient to narrow down causes of connection failure. Use the information to work out whether configuration settings are incorrect or if the required components or services are unavailable.

For instructions about using the Secure Gateway Diagnostics tool, see "Viewing a Secure Gateway Diagnostics Report" on page 126.

Examining the Secure Gateway Application Log

Careful examination of the Secure Gateway event log can help you identify the sources of system problems. For example, if log warnings show that the Secure Gateway failed because it could not locate the specified certificate, you can conclude that the certificate is missing or installed in the wrong certificate store. In general, information in the event log helps you trace a record of activity leading up to the event of failure.

For a complete list of error and event messages for the Secure Gateway, see “Error Messages” on page 171.

Common Problems

The following sections describe known system problems and preventive measures and possible solutions to resolve them.

Installation and Upgrade Problems

Installer Does not Remember Selections if You Cancel Installation and Relaunch the Installer

If you cancel the installation of Secure Gateway components before the installation is complete, the Secure Gateway installer does not save any settings or values entered.

This is the default behavior of Secure Gateway installer; that is, if you cancel or abort Secure Gateway installation, the selections you made prior to cancelling the install are not saved.

Important Citrix recommends that you uninstall and reinstall Secure Gateway components if you cancel or abort an installation.

Error Message “Unable to stop the World Wide Web Publishing Service” Appears When the STA Installation Completes

This error message appears if a service dependent on the World Wide Web Publishing Service is running during the installation. To prevent this conflict, ensure all services dependent on the World Wide Web Publishing Service are stopped or disabled before you install the STA.

Certificate Problems

Secure Gateway Fails with a CSG1213 Error

This error implies that SChannel was unable to validate certificate credentials of the server certificate used by the Secure Gateway.

Ensure that the certificate installed was issued by a trusted source, is still valid, and is issued for the correct machine.

To check your certificates

1. Log on as an administrator to the server running the Secure Gateway.
2. Click **Start > Programs > Citrix > Secure Gateway > Secure Gateway Service Configuration**.
3. On the **Select configuration level** screen, select **Advanced**.
4. In the **Select server certificate** dialog box, select the certificate the Secure Gateway is configured to use and click **View**.
5. Examine the server certificate.
6. Check that the value in the **Issued To** field matches the FQDN of this server
7. When you view the certificate, ensure that it contains a key icon and the caption **"You have private key that corresponds to this certificate"** at the bottom of the **General** tab. The lack of an associated private key can result in the CSG1213 error.
8. Ensure the certificate is not expired. If it is expired, you need to apply for certificate renewal.

Contact your Corporate Security department for assistance with certificate renewal.

Connection Problems

Client Connections Launched from IP Addresses in the Logging Exclusions List Fail

For security reasons, IP addresses configured in the logging exclusions list are not allowed to establish connections to the Secure Gateway.

The logging exclusions list is designed to help keep the system log free of redundant data. You can configure the IP address of load balancing devices in the Logging Exclusions list. Configuring an exclusions list enables the Secure Gateway to ignore polling activity from such devices and keeps the log free of this type of data.

As a preventive security measure, devices configured in the Logging Exclusions list are not allowed to establish connections to the Secure Gateway. This measure blocks connections to the Secure Gateway that do not leave an audit trail.

Load Balancers do Not Report Active Client Sessions if They Are Idle

Some load balancers stop reporting active client connections flowing through them if the connections are idle for a while because of the way in which certain load balancers treat idle connections.

Connections that are idle for a certain amount of time stop being represented as active connections in the load balancer's reporting tools even though they are still valid connections.

You can resolve this issue by modifying the keep–alive settings in the Windows registry on the server(s) running the Secure Gateway.

If you have a load balanced an array of servers running the Secure Gateway, decrease the keep–alive values to force packets to be sent after a period of session inactivity. For more information about configuring TCP/IP keep–alive settings, see "Connection Keep–Alive Values and the Secure Gateway" on page 140.

Auto Client Reconnect Dialog Appears Repeatedly on the Client Device

Users connected to published applications or resources available on a server farm may experience this problem if your Secure Gateway deployment contains an NFuse Classic 1.7 server. This problem does not occur if you are using the Web Interface.

For security reasons, the Secure Gateway does not support the Auto Client Reconnect feature available in the MetaFrame Presentation Server Client for 32-bit Windows.

The client displays correct behavior; that is, continues to attempt reconnection and displays the reconnection count down dialog box.

If your users find this behavior confusing or disruptive, consider disabling auto client reconnect on the client device. For more information, see the *Client for 32-bit Windows Administrator's Guide*, available from the Document Center.

Performance Issues with Transferring Files between a Client and a Computer Running MetaFrame Presentation Server

When connecting to MetaFrame XP with Feature Release 2 or later servers, users may experience performance issues with data transfer using client drive mapping on high bandwidth, high latency connections.

As a workaround, you can optimize throughput by increasing the value of TcpWindowSize in the Windows registry of your server running the Secure Gateway.

To modify this setting, edit the following Windows Registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip
\Parameters\TcpWindowSize
```

Citrix recommends setting the value of TCPWindowSize to 0xFFFF(64K).

Warning Using the Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee resolution of problems resulting from the incorrect use of Registry Editor. Use Registry Editor at your own risk

Be aware that this change incurs higher system memory usage. Citrix recommends increasing physical system memory on the server running the Secure Gateway to suit the typical usage profile of the network.

For more information, refer to the Microsoft Knowledgebase Article "TCP/IP and NBT Configuration Parameters for Windows 2000 or Windows NT (Q120642)" available from the Microsoft Support Web site at http://support.microsoft.com/support/kb/articles/.

Other Problems

Failed Client Connections to the Secure Gateway Result in Duplicate Entries in the Secure Gateway Log

You may find duplicate entries for client connection attempts in the Secure Gateway application and performance logs. Duplicate entries can occur in the following situations:

- SSL protocol mismatch between the client device and the server running the Secure Gateway
- Client automatically attempts to reconnect if the first connection attempts fails

Though it may appear so, the log entries are not really duplicates but a record of client behavior. In the above cases, the client attempts to reconnect if it fails the first time.

Application Log for the STA Is Empty or Missing

Microsoft guidelines for securing Web servers recommends removing access privileges to the \inetpub\scripts\ directory.

The STA is an ISAPI DLL that is loaded and called by IIS. If you removed access rights to the directory in which the STA system files reside, IIS is unable to load and execute the STA. As a result of insufficient access privileges, the STA is unable to read its configuration file and/or write to its log file.

The STA is designed to log fatal errors to its application log, *stayyyymmdd-xxx*.log, which is located in the \inetpub\scripts directory. However, if the STA lacks write privileges to the \scripts directory, it may not be successful in creating a log file.

To check directory access privileges in IIS

To ensure that the directory where you installed the STA has sufficient read and execute permissions in IIS, do the following:

1. Click **Start > Programs > Administrative Tools > Internet Services Manager**.
2. In the **Internet Services Manager** console, check that the **Scripts** directory exists and is not reporting an error.
3. Right-click **Scripts** and select **Properties**. Check the following:
   - On the **Virtual Directory** tab, ensure **Execute Permissions** is set to **Scripts and Executables**.
   - On the **Directory Security** tab, ensure **Anonymous access** is enabled.
4. Close Internet Services Manager.
5. Stop and restart the World Wide Web Publishing Service to let the changes take effect.

If the STA log file is empty, ensure that logging is enabled on the STA.

To enable the STA to log errors

1. Modify the ctxsta.config file, located in \inetpub\scripts, and specify appropriate values for the **LogDir** and **LogLevel** parameters.
2. Ensure that the directory value specified for LogDir has sufficient access permissions under IIS.
3. After you modify the configuration file, stop and restart the World Wide Web Publishing Service.
4. To ensure that you receive complete details of STA events, Citrix recommends setting LogLevel to 3; this ensures details of every event that occurs are recorded.

When the STA is working and optimized, consider setting LogLevel to a value best suited to your needs.

If You Are Still Unable to Resolve the Problem

If you are still experiencing problems with a Secure Gateway deployment, see the Citrix Web site, http://www.citrix.com/support/, for available technical support options.

About Digital Certificates

This appendix provides conceptual information about the security technologies used in the Secure Gateway solution, helps you identify the number and type of certificates required, and helps you decide how and where to obtain and install them. This appendix contains the following topics:

- Understanding SSL/TLS, Cryptography, and Digital Certificates
- Getting Certificates
- Server Certificates
- Root Certificates

Understanding SSL/TLS, Cryptography, and Digital Certificates

This section introduces the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, and provides an overview of cryptography and Public Key Infrastructure (PKI).

SSL and TLS

SSL and TLS are the leading Internet protocols providing security for e-commerce, Web services, and many other network functions.

The SSL protocol is today's standard for securely exchanging information on the Internet. Originally developed by Netscape, the SSL protocol became crucial to the operation of the Internet. As a result, the Internet Engineering Taskforce (IETF) took over responsibility for the development of SSL as an open standard. To clearly distinguish SSL from other ongoing work, the IETF renamed SSL as TLS. The TLS protocol is the descendant of the third version of SSL; TLS 1.0 is identical to SSL 3.1.

Some organizations, including US government organizations, require the use of TLS to secure data communications. These organizations may also require the use of validated cryptography. FIPS (Federal Information Processing Standard) 140 is a standard for cryptography.

The SSL/TLS protocol allows sensitive data to be transmitted over public networks such as the Internet by providing the following important security features:

Authentication. A client can determine a server's identity and ascertain that the server is not an impostor. Optionally, a server can also authenticate the identity of the client requesting connections.

Privacy. Data passed between the client and server is encrypted so that if a third party intercepts messages, it cannot unscramble the data.

Data Integrity. The recipient of encrypted data knows if a third party corrupts or modifies that data.

Cryptography

The SSL/TLS protocol uses *cryptography* to secure communications. Cryptography provides the ability to encode messages to ensure confidentiality. Cryptography is also used to authenticate the identity of a message source and to ensure the integrity of its contents.

A message is sent using a secret code called a *cipher*. The cipher scrambles the message so that it cannot be understood by anyone other than the sender and receiver. Only the receiver who has the secret code can decipher the original message, thus ensuring confidentiality.

Cryptography allows the sender to include special information in the message that only the sender and receiver know. The receiver can authenticate the message by reviewing the special information.

Cryptography also ensures that the contents of a message are not altered. To do this, the sender includes a cryptographic operation called a *hash function* in the message. A hash function is a mathematical representation of the information, similar to the checksums found in communication protocols. When the data arrives at its destination, the receiver calculates the hash function. If the receiver's hash function value is the same as the sender's, the integrity of the message is assured.

Types of Cryptography

There are two main types of cryptography:

- Secret key cryptography
- Public key cryptography

In cryptographic systems, the term *key* refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information.

Secret key cryptography is also known as *symmetric key cryptography*. With this type of cryptography, both the sender and the receiver know the same secret code, called the *key*. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key.

This method works well if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers of people. In addition, there is also the problem of how you communicate the secret key securely.

Public key cryptography, also called *asymmetric encryption*, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched *public* and *private* keys.

The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Because these keys work only as a pair, encryption initiated with the public key can be decrypted only with the corresponding private key, and vice-versa. The following example illustrates how public key cryptography works:

1. Ann wants to communicate secretly with Bill. Ann encrypts her message using Bill's public key (which Bill made available to everyone) and Ann sends the scrambled message to Bill.
2. When Bill receives the message, he uses his private key to unscramble the message so that he can read it.

3. When Bill sends a reply to Ann, he scrambles the message using Ann's public key.
4. When Ann receives Bill's reply, she uses her private key to unscramble his message.

The major advantage asymmetric encryption offers over symmetric key cryptography is that senders and receivers do not have to communicate keys up front. Provided the private key is kept secret, confidential communication is possible using the public keys.

Combining Public Key and Secret Key Cryptography. The main disadvantage of public key cryptography is that the process of encrypting a message, using the very large keys common to PKI, can cause performance problems on all but the most powerful computer systems. For this reason, public key and secret key cryptography are often combined. The following example illustrates how this works:

1. Bill wants to communicate secretly with Ann, so he obtains Ann's public key. He also generates random numbers to use just for this session, known as a *session key*.
2. Bill uses Ann's public key to scramble the session key.
3. Bill sends the scrambled message and the scrambled session key to Ann.
4. Ann uses her private key to unscramble Bill's message and extract the session key.

When Bill and Ann successfully exchange the session key, they no longer need public key cryptography—communication can take place using just the session key. For example, public key encryption is used to send the secret key; when the secret key is exchanged, communication takes place using secret key encryption.

This solution offers the advantages of both methods—it provides the speed of secret key encryption and the security of public key encryption.

Digital Certificates and Certificate Authorities

In the above scenarios, how can Ann be sure that Bill is who he says he is and not an impostor? When Ann distributes her public key, Bill needs some assurance that Ann is who she says she is.

The ISO X.509 protocol defines a mechanism called a *certificate* that contains a user's public key that has been signed by a trusted entity called a *certificate authority* (CA).

Certificates contain information used to establish identities over a network in a process called *authentication*. Like a driver's licence, a passport, or other forms of personal identification, certificates enable servers and clients to authenticate each other before establishing a secure connection.

Certificates are valid only for a specified time period; when a certificate expires, a new one must be issued. The issuing authority can also revoke certificates.

To establish an SSL/TLS connection, you require a server certificate at one end of the connection and a root certificate of the CA that issued the server certificate at the other end.

Server certificate. A server certificate certifies the identity of a server. The type of digital certificate that is required by the Secure Gateway is called a *server certificate*.

Root certificate. A root certificate identifies the CA that signed the server certificate. The root certificate belongs to the CA. The type of digital certificate required by a client device to verify the server certificate is called a *root certificate*.

When establishing an SSL connection with a Web browser on a client device, the server sends its certificate to the client.

When receiving a server certificate, the Web browser (for example, Internet Explorer) on the client device checks to see which CA issued the certificate and if the CA is trusted by the client. If the CA is not trusted, the Web browser prompts the user to accept or decline the certificate (effectively accepting or declining the ability to access this site).

Now when Ann receives a message from Bill, the locally stored information about the CA that issued the certificate is used to verify that it did indeed issue the certificate. This information is a copy of the CA's own certificate and is referred to as a root certificate.

Certificates generally have a common format, usually based on ITU standards. The certificate contains information that includes the:

Issuer. The organization that issues the certificates.

Subject. The party that is identified by the certificate.

Period of validity. The certificate's start date and expiration date.

Public key. The subject's public key used to encrypt data.

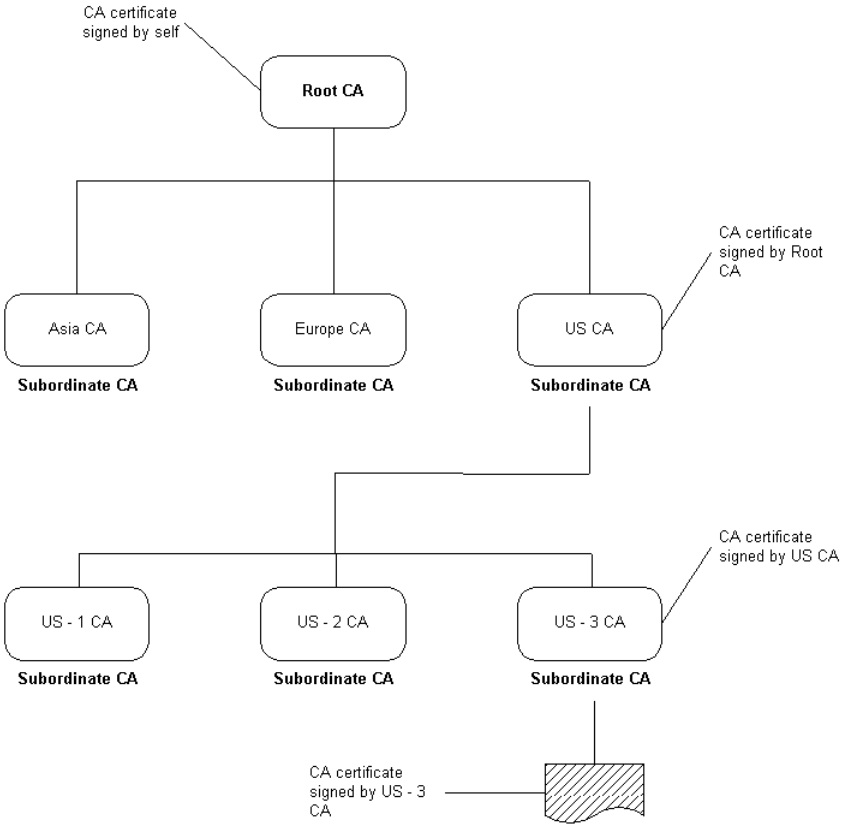
Issuer's signature. The CA's digital signature on the certificate used to guarantee its authenticity.

A number of companies and organizations currently act as CAs, including VeriSign, Baltimore, Entrust, and their respective affiliates.

Certificate Chains

Some organizations delegate the responsibility for issuing certificates to resolve the issue of geographical separation between organization units, or that of applying different issuing policies to different sections of the organization.

Responsibility for issuing certificates can be delegated by setting up subordinate CAs. The X.509 standard includes a model for setting up a hierarchy of CAs. In this model, the root CA is at the top of the hierarchy and has a self-signed certificate. The CAs that are directly subordinate to the root CA have CA certificates signed by the root CA. CAs under the subordinate CAs in the hierarchy have their CA certificates signed by the subordinate CAs.



This illustration shows the hierarchical structure of a typical digital certificate chain.

CAs can sign their own certificates (that is, they are self-signed) or they can be signed by another CA. If the certificate is self-signed, they are called *root* CAs. If they are not self-signed, they are called *subordinate* or *intermediate* CAs.

If a server certificate is signed by a CA with a self-signed certificate, the certificate chain is composed of exactly two certificates: the end entity certificate and the root CA. If a user or server certificate is signed by an intermediate CA, the certificate chain is longer.



This illustration shows a typical digital certificate chain. The first two elements are the end entity certificate (in this case, gwy01.company.com), and the certificate of the intermediate CA, in that order. The intermediate CA's certificate is followed by the certificate of its CA. This listing continues until the last certificate in the list is for a root CA. Each certificate in the chain attests to the identity of the previous certificate.

Certificate Revocation Lists

From time to time, CAs issue certificate revocation lists (CRLs). CRLs contain information about certificates that can no longer be trusted. For example, suppose Ann leaves XYZ Corporation. The company can place Ann's certificate on a CRL to prevent her from signing messages with that key.

Similarly, you can revoke a certificate if a private key is compromised or if that certificate expired and a new one is in use. Before you trust a public key, make sure that the certificate does not appear on a CRL.

Certificate Expiration and Renewal

Certificates are issued with a planned lifetime and explicit expiration date. After it is issued, a certificate is considered valid until its expiration date is reached. After the expiration date is past, the certificate cannot be used to validate a user session. This policy improves security by limiting the damage potential of a compromised certificate. These expiration dates are set by the CA that issued the certificate.

Usually, you need to renew a certificate before it expires. Most CAs offer a well documented process for certificate renewal. Consult the Web site of your CA for detailed instructions about renewing certificates.

Getting Certificates

When you identify the number and type of certificates required for your Secure Gateway deployment, you must decide where to obtain the certificates. Where you choose to obtain certificates depends on a number of factors, including:

- Whether or not your organization is a CA, which is likely to be the case only in very large corporations
- Whether or not your organization has already established a business relationship with a public CA
- The fact that the Windows operating system includes support for many public Certificate Authorities
- The cost of certificates, the reputation of a particular public CA, and so on

If Your Organization Is Its Own Certificate Authority

If your organization is running its own CA, you must determine whether or not it is appropriate to use your company's certificates for the purpose of securing communications in your Secure Gateway installation. Citrix recommends that you contact your corporate security department to discuss this and to get further instructions about how to obtain certificates.

If you are unsure if your organization is a CA, contact your corporate security department or your organization's security expert.

If Your Organization Is Not Its Own Certificate Authority

If your organization is not running its own CA, you need to obtain your certificates from a public CA such as VeriSign.

Obtaining a digital certificate from a public CA involves a verification process in which:

- Your organization provides corporate information so the CA can verify that your organization is who it claims to be. The verification process may involve other departments in your organization, such as accounting, to provide letters of incorporation or similar legal documents.
- Individuals with the appropriate authority in your organization are required to sign legal agreements provided by the CA.
- The CA verifies your organization as a purchaser; therefore your purchasing department is likely to be involved.
- You provide the CA with contact details of suitable individuals who they can call if there are queries.

Server Certificates

Your organization's security expert should have a procedure for obtaining server certificates. Instructions for generating server certificates using various Web server products are available from the Web sites of popular CAs such as Verisign and others.

Tip Several CAs offer Test Server Certificates for a limited trial period. It might be expedient to obtain a Test Certificate to test the Secure Gateway before deploying it in a production environment. If you do this, be aware that you need to download matching Test Root Certificates that must be installed on each client device that connects through the Secure Gateway.

Obtaining and Installing Server Certificates

To provide secure communications (SSL/TLS), a server certificate is required on the server running the Secure Gateway. The steps required to obtain and install a server certificate on a server running the Secure Gateway are as follows:

1. Create a certificate request.
2. Apply for a server certificate from a valid CA.
3. Save the certificate response file sent by the CA as an X.509 Certificate (.cer format).
4. Import the X.509 certificate into the certificate store.
5. Export the certificate into Personal Information Exchange format (.pfx, also called PKCS #12).
6. Install the server certificate on the server running the Secure Gateway.

Each of the above steps is described in the following sections.

To create a certificate request

Create a certificate request using the IIS Certificate wizard on any Windows 2000 server that has IIS installed. To do this:

1. Click **Start > Programs > Administrative Tools > Internet Services Manager**.
2. On the Internet Information Services console, right-click the entry for **Default Web Site** and select **Properties**.
3. From the **Default Web Site Properties** screen, click the **Directory Security** tab.
4. Click **Server Certificate** under **Secure Communications**.

5. The IIS Server Certificate wizard appears. Click **Next**.
6. Select **Create a new certificate** and click **Next**.
7. Select **Prepare the request now, but send it later**. Click **Next**.
8. In **Name**, type the name for the server certificate.
9. In **Bit Length**, enter the bit length to be used for the certificate's encryption strength. The greater the bit length, the higher the security. Citrix recommends that you select 1024 or higher. If you are specifying a bit length higher than 1024, ensure that the Clients deployed support it. For information about supported encryption strength on an client device, see the appropriate client's Administrator's Guide.

   Click **Next**.
10. Enter details about your organization. Click **Next**.
11. Enter the FQDN of the server running the Secure Gateway and click **Next**.
12. In **Geographical Information**, enter pertinent geographical information about your location. Click **Next**.
13. Save the certificate request as a text file; for example, certreq.txt. Click **Finish** to exit the wizard.

Important Part of an initial request for a certificate involves generating a public/private key pair that is stored on your server. Because the public key from this key pair is encoded in your certificate, loss of the key pair on your server renders your certificate worthless. Make sure you back up your key pair data on another computer, a floppy disk, or both. The Microsoft IIS Key Manager has a special Export Key function that can be used to generate a backup file.

To apply for a server certificate

To apply for a valid server certificate, follow the process specified by the public or private CA you are using.

To save the certificate response file

The duration of the certification process can vary, but when the process is complete, you receive a response file from the CA. The response file contains the public key that is signed by the CA.

Copy the text block that contains the public key and save it to an X.509 format certificate file; *filename.cer*.

```
------BEGIN CERTIFICATE------
MIIDBDCCAq4CEGTFq6PjvXhFUZjJKoZIhvcNAQEEBQAwgakxFjAU
BgNVBAoTDVZlcmlTaWduLCBJbmMxRzBFBgNVBAsTPnd3dy52ZXJpc2lnbi5jb20vcmVwb
3NpdG9yeS9UZXN0Q1BTIEluY29ycC4gQnkgUmVmLiBMaWFiLiBMVEQuMUYwRAYDV
QQLEz1Gb3IgVmVyaVNpZ24gYXV0aG9yaXplZCB0ZXN0aW5nIG9ubHkuIE5vIGFzc3VyY
W5jZXMgKEMpVlMxOTk3MB4XDTAyMDIwNDAwMDAwMFoXNCtQsSw+wa04zsadIcnDT
KDFL64ihQfdu4gVqK8o86IzEPfoglOBGGmMMO4aecyg8XPqBtG3ghDaTZsz49KBPUiduIGlq
1BNVOi0IzzwWHkkKNIaaLuWWQH6ZpwRAqgrr2VVzT97FGC34nEtcvlYQ3bP8rSyz5f34kY
e786kplRvDGiuDgyIttLcoHWZxZz2Tbba5h55mxuHKm4EWG7bM54T1nTErJbdkCAwEAATA
NBgkqhkiG9w0BAQQFAANBAKNuQQmhVOjuefCtrALFtlM576smD65rYraQ8i8aNI76wZdC
ue2XgKLzRSvfIz0ylt81HCGhgHA=
------END CERTIFICATE------
```

To import the X.509 certificate

When you import a certificate, you copy the certificate from a file that uses a standard certificate storage format to a certificate store for your computer account.

Important Do not attempt to import the file by double-clicking or right-clicking the certificate file within Windows Explorer. Doing so places the certificate in the certificate store for the current user.

The server certificate must be placed in the certificate store for the Local Computer. Use the Certificate Import wizard to install the server certificate. To import the certificate:

1. Log on to the system as an administrator.
2. Click **Start**, click **Run**, type **mmc**, and then click **OK**.
3. On the **Console** menu, click **Add/Remove Snap-in**, and then click **Add**.
4. Under **Snap-in**, double-click **Certificates**, click **Computer account**, and then click **Next**.
5. In the **Select Computer** dialog box, select **Local computer**, and click **Finish**.
6. Click **Close** in the **Add Standalone Snap-in** dialog box.
7. Click **OK** to close the **Add/Remove Snap-in** dialog box.
8. In the console tree, select **Certificates (Local Computer)** > **Personal**.
9. From the **Action** menu, choose **All Tasks** > **Import**.
10. Perform the following actions:

- Browse to and select the file containing the certificate you are importing.
- Select if you want the certificate to be placed automatically in a certificate store (based on the type of certificate), or if you want to be able to specify where the certificate is stored.

The certificate; *filename.cer*, is now imported and stored in the local certificate store.

To export the server certificate

Before you can install the server certificate on the server running the Secure Gateway, you must export the certificate to PKCS #12 (Personal Information Exchange Syntax Standard) format. The PKCS #12 standard specifies a portable format for storing or transporting a user's private keys, certificates, and so on.

Important Part of generating a key pair is specifying a password used to encrypt it. This prevents someone with access to the keypair data from extracting the private key and using it to decrypt SSL/TLS traffic to and from your server. Forgetting this password could render your certificate worthless, so be sure to remember it and save it in a secure location.

To export the certificate:

1. Launch the **Microsoft Management Console** and load the snap-in for **Certificates**.
2. The **Certificates snap-in** dialog box appears; select **Computer Account** and click **Next**.
3. The **Select Computer** dialog box appears; select **Local Computer** and click **Finish**.
4. Click **Close** and then **OK**.
5. In the console tree, Select **Certificates** > **Personal** > **Certificates**. A list of available certificates appears in the right pane.
6. In the **Details** pane, click the certificate you want to export.
7. From the **Action** menu, choose **All Tasks** > **Export**. The Certificate Export wizard screen appears. Click **Next**.
8. In the **Export Private Key** dialog box, select **Yes**, **export the private key**. (This option appears only if the private key is marked as exportable and you have access to the private key.) Click **Next**.
9. In the **Export File Format** dialog box:
   - Select the **Include all certificates in the certification path if possible** check box.

- Select the **Enable strong protection** check box.
- Clear the **Delete the private key if the export is successful** check box.

Click **Next**.

10. In the **Password** dialog box, type a password to protect the private key you are exporting. Take precautions to keep the specified password safe because you are required to enter this password when you install the certificate. Click **Next**.
11. In the **File to Export** dialog box, type a file name and path for the PKCS #12 file that stores the exported certificate and private key. Click **Next**.
12. Click **Finish** to complete certificate export.

Note When the Certificate Export wizard is finished, the certificate remains in the certificate store in addition to being in the newly created file. To remove the certificate from the certificate store, you must delete it.

To install the server certificate

The final step in the process is to install the PKCS #12 file on the server running the Secure Gateway.

Important Do not attempt to import the PFX file by double-clicking or right-clicking the certificate file within Windows Explorer. Doing so places the certificate in the certificate store for the current user.

The server certificate must be placed in the certificate store for the Local Computer. Instead, use the Certificate Import Wizard to install the server certificate. To do this:

1. Copy the PKCS #12 file, *filename.pfx*, to the server running the Secure Gateway.
2. Open an MMC console that contains the Certificates snap-in.
3. The **Certificates snap-in** dialog box appears; select **Computer Account** and click **Next**.
4. The **Select Computer** dialog box appears; select **Local Computer** and click **Finish**.
5. Click **Close** and then **OK**.
6. In the console tree, select **Certificates** > **Personal**.
7. From the **Action** menu, choose **All Tasks** > **Import**.
8. In the **Certificate Import** wizard do the following to import your PFX file:
   - Browse to and select the file containing the certificate you are importing.

- Type the password used to encrypt the private key.
- Select if you want the certificate to be placed automatically in a certificate store (based on the type of certificate), or if you want to be able to specify where the certificate is stored.

The certificate, *filename.pfx*, is now imported and stored in the local certificate store.

Root Certificates

A root certificate must be present on every client device that connects to the secure network through the Secure Gateway.

Support for most trusted root authorities is already built into the Windows operating system and Internet Explorer. Therefore, there is no need to obtain and install root certificates on the client device if you are using these CAs. However, if you decide to use a different CA, you need to obtain and install the root certificates yourself.

Obtaining a Root Certificate from a CA

Root certificates are available from the same CAs that issue server certificates. Well-known or trusted CAs include Verisign, Baltimore, Entrust, and their respective affiliates.

CAs tend to assume that you already have the appropriate root certificates (this is because most Web browsers have root certificates built-in as standard) so you need to specifically request the root certificate.

Several types of root certificates are available. For example, VeriSign has approximately 12 root certificates that they use for different purposes, so it is important to ensure that you obtain the correct root certificate from the CA.

Installing Root Certificates on a Client Device

To install a root certificate on a client device

1. Double-click the root certificate file. The root certificate file has the extension .cer, .crt, or .der.
2. Verify that you are installing the correct root certificate.
3. Click **Install Certificate**.
4. The Certificate Import wizard starts. Click **Next**.
5. Choose the **Place all certificates in the following store** option and then click **Browse**.
6. On the **Select Certificate Store** screen, select **Show physical stores**.
7. Expand the Trusted Root Certification Authorities store and then select **Local Computer**. Click **OK**.
8. Click **Next** and then click **Finish**. The root certificate is installed in the store you selected.

For information about root certificate availability and installation on platforms other than 32-bit Windows, refer to product documentation appropriate for the operating system you are using.

Error Messages

This appendix describes the system, error, warning, and informational messages that are recorded in the application log for the Secure Gateway.

This appendix contains the following topics:

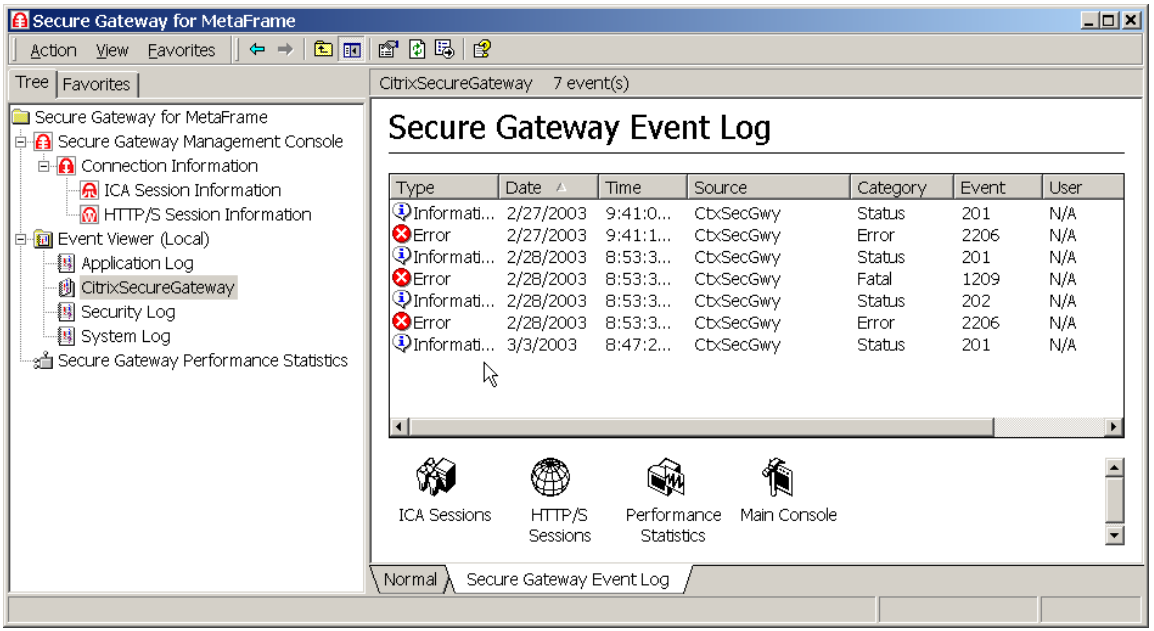
- Checking for Error Messages
- Secure Gateway Service Messages
- Logon Agent Messages
- STA Messages

Checking for Error Messages

Secure Gateway error messages are logged to the Secure Gateway application log. Use the Windows Event Viewer to view Secure Gateway error messages.

To view Secure Gateway error messages

1. Click **Start > Programs > Citrix > Secure Gateway > Secure Gateway Management Console**.
2. Expand the Event Viewer node and click **CitrixSecureGateway**. A list of all errors and events recorded since the service was started appear.



This illustration shows the Secure Gateway Event Log.

Double-click an event to view its **Properties**. The **Description** field contains the event ID and a brief description of the Secure Gateway error. For example, CSG0201 is the ID of the event that occurs when the Secure Gateway is started. The Event ID and description can be used by Citrix support representatives to troubleshoot system problems.

Secure Gateway Service Messages

Status Messages

This section contains system messages that are logged when a normal operational event such as starting or stopping the service occurs.

Error Number	Error Message	Description
CSG0200	Reserved	Message is reserved for system use.
CSG0201	Secure Gateway Service started.	The service started successfully.
CSG0202	Secure Gateway Service stopped.	The service was stopped.
CSG0203	Secure Gateway Service paused.	The service is paused by the Windows Service Control Manager.
CSG0204	Secure Gateway Service resumed.	The service is resumed, after having been paused, by the Windows Service Control Manager.
CSG0205	Secure Gateway Service paused as active connections reached limit of *maxconn*.	The service is paused because the number of active connections has reached the maximum limit. *maxconn* is replaced by the current value of Maximum Connections.
CSG0206	Secure Gateway Service resumed as active connections is less than or equal to *connresume*.	The service is resumed after being paused as a result of event specified by CSG0205; *connresume* is replaced by the value specified in Connection Resume. The service is resumed because the number of active connections dropped to the current value specified in Connection Resume.

Fatal Error Messages

Fatal error messages are logged as a result of operational failure that prevents the the Secure Gateway from starting. To resolve issues arising out of fatal errors, ensure your user account has the required administrative privileges.

Error Number	Error Message	Description
CSG1200	Reserved.	Message is reserved for system use.
CSG1201	Unable to initialize system.	The service is unable to start because of an operational failure such as allocation of memory, starting worker threads, and so on. The server running the Secure Gateway must be reserved for the exclusive use of the Secure Gateway. If you are running other applications, remove them from the system before restarting the service.
CSG1202	Insufficient memory to initialize system.	The service is unable to start because insufficient memory is available. Increase available system memory and remove all other applications from this server.
CSG1203	Registry entries to configure service [*service name*] not found.	The service failed to start because registry entries required to start the service could not be found. It appears that your installation is corrupted. Uninstall and reinstall the Secure Gateway.
CSG1204	Insufficient privileges to access registry entries for service [*service name*].	The service failed to start because of insufficient access privileges to access registry entries. Uninstall and reinstall the Secure Gateway. Ensure that you have administrative privileges.
CSG1205	Invalid or missing configuration value [*value*] in registry section [*section name*].	The service failed to start because a configuration parameter is missing from the registry section. Your registry appears to be corrupted. Uninstall and reinstall the Secure Gateway.
CSG1206	Invalid configuration value [*value*] in registry section [*section name*].	The service encountered an invalid configuration value in the registry and could not start. Reconfigure the Secure Gateway.
CSG1207	Missing configuration value [*value*] in registry section [*section name*].	The service encountered a missing configuration value in the named registry section and could not start. Reconfigure the Secure Gateway.
CSG1208	Missing configuration section in registry for [*section name*].	The service encountered a missing configuration section in the registry and could not start. Reconfigure the Secure Gateway.

Error Number	Error Message	Description
CSG1209	Unable to bind to IP interface [*IP address:port*].	The service is unable to bind to the interface because the IP address and port specified are in use. Configure the conflicting application or service to use a different IP address and port. For example, IIS may be configured to listen on port 443.
CSG1210	Unable to listen on IP interface [*IP address:port*].	The service is unable to listen on the interface specified because it is in use. Configure the conflicting application or service to use a different IP address and port.
CSG1211	Unable to open local certificate store.	The service could not open the local certificate store to retrieve certificates. Your operating system is missing a local certificate store. Repair or reinstall the operating system on this server.
CSG1212	Unable to find certificate specified by [*FQDN*].	The service could not find a certificate in its local certificate store for the specified *FQDN.* Ensure you install the specified certificate and that your user account has sufficient user privileges to access the local certificate store.
CSG1213	SChannel returned error: Unable to acquire certificate credentials.	The service is unable to initialize SChannel on Windows. Check the certificate date and validity. If required, acquire a new certificate.
CSG1214	Certificate specified by [*FQDN*] is not valid for current date.	The service determined that the certificate date is not valid for the current system date. Check the certificate date and validity. If required, acquire a new certificate.

Service Error Messages

These error messages are logged as a result of partial failure of the Secure Gateway.

Error Number	Error Message	Description
CSG2200	Undefined error.	Message reserved for system use.
CSG2201	Unable to initialize performance counters.	The service is unable to access memory for performance counters. Performance counter data is not updated.
CSG2202	Error accepting connection from client [*IP address]*. Connection dropped.	The service is unable to complete the connection request from the client due to a TCP/IP error, an operating system error, and so on. Try stopping and restarting the service and/or reboot your server.
CSG2203	Insufficient memory to establish connection for client [*IP address]*.	The service is running low on memory and is unable to allocate sufficient memory to initialize a connection for this client IP address. Increase system memory or close unnecessary applications and services.
CSG2204	Unable to connect to STA or Authentication Service [*IP address]* for client IP [*IP address]*.	The service is unable to establish a connection to the authority server specified by *IP address* for this *client IP*. Ensure this server is able to contact servers running the STA or Authentication Service. Also ensure that the STA or the Authentication is installed and running on the specified server(s).
CSG2205	STA or Authentication Service [*Authority ID*] is unknown, unable to satisfy validation request for client IP [*IP address*].	The service cannot resolve the unique identifier for the authority server specified, and is unable to complete the validation request for the client. Reconfigure the Secure Gateway and enter correct details of the server running the STA or the Authentication Service.
CSG2206	Unable to resolve address for [*Server Identifier]* in the registry section [*Section Name]*.	The service is unable to resolve the address for the entry, in the registry section called *Section Name*. Ensure the entry can be resolved by the DNS or add an entry to the local hosts file.

Warning Messages

These messages are logged as a result of events caused by corrupted data requests or data packets received, ticket timeouts, and so on.

Error Number	Error Message	Description
CSG3200	Warning undefined.	Message is reserved for system use.
CSG3201	Client IP [*IP address*] connection dropped due to internal processing error specified by [*hex value*].	An internal service error occurred. The connection is dropped.
CSG3202	Client IP [*IP address*] connection dropped, connection timed out.	The service dropped the connection due to insufficient information from the client. This error could be either due to poor network performance, an attacker attempting a DOS attack, or a user error.
CSG3203	Client IP [*IP address*] sent invalid HTTP, connection dropped.	The service dropped the client connection because the requested data is not recognized.
CSG3204	Client IP [*IP address*] sent bad cookie [*STA session ticket or Authentication Service access token*], connection dropped.	Data received from the client is not recognized.
CSG3205	Unable to parse data from STA or Authentication Service [*Authority ID*] specified by internal error [*error message from a HTTP or XML parser*], client IP [*IP address*] connection dropped.	The server running the STA or Authentication Service responded with an error. Ensure that the STA or the Authentication Service is installed and running on the specified server(s).
CSG3206	Service received HTTP error [*error message from a HTTP or XML parser*] from STA or Authentication Service [*Authority ID*], client IP [*IP address*] connection dropped.	The server running the STA or Authentication Service responded with an error. Ensure that the STA or the Authentication Service is installed and running on the specified server(s).
CSG3207	Service received error [*error message*] from STA or Authentication Service [Authority ID], Client IP [*IP address*] connection dropped.	The STA or Authentication Service responded with an error. The *error message* text may provide more information about resolving this problem.
CSG3208	Unable to resolve name [*server*], client IP [*IP address*] connection dropped.	The service is unable to resolve the server name specified by the client, connection failed. Ensure the entry can be resolved by the DNS or add an entry to the local hosts file.
CSG3209	Connection refused, client IP [*IP address*] is not allowed by inbound access control list.	The service refused the connection because its inbound ACL does not contain an entry for the client IP address.

Error Number	Error Message	Description
CSG3210	Authentication Service [*Authentication Service ID*] does not allow access to server [*IP address:port*], connection from client IP [*IP address*] dropped.	The service refused the connection because the access center does not allow a connection to the requested resource.
CSG3211	Client IP [*IP address*] sent invalid signature of [*hex value*], connection dropped.	The service refused the connection because data received is not recognized as valid.
CSG3212	Client IP [*IP address*] sent invalid command of [*hex value*], connection dropped.	The service refused the connection because data received is not recognized as valid.
CSG3213	Client IP [*IP address*] sent unexpected data of [*hex value*], connection dropped.	The service refused the connection because data received is not recognized as valid.
CSG3214	Server [*name*] refused SSL or TLS connection from service for client IP [*IP address*].	The service refused the connection because SSL handshake with the destination server failed.
CSG3215	Cannot connect to server [*name*], which returned a certificate with the name [*server name*] which does not match.	The service refused the connection because the server name is different from the server name in the certificate.
CSG3216	Cannot connect to server [*name*], which returned a certificate with a bad chain of trust.	The service does not trust the certificate returned by the server. Install a valid certificate on the server or an appropriate root authority on the server running the Secure Gateway.
CSG3217	Cannot connect to server [*name*], client IP [*IP address*] connection dropped.	The service could not contact the server specified.
CSG3218	Outbound access control list does not allow connection to server [*name*], client IP [*IP address*] connection dropped.	The outbound ACL on the Secure Gateway does not have an entry for the requested server.
CSG3219	Client IP [*IP address*] connection, terminated by the administrator through MMC.	The client connection is terminated by the administrator through the Secure Gateway Management Console.
CSG3220	Client IP [*IP address*] attempted an ICA connection, current gateway installation mode does not allow ICA connections.	The Secure Gateway is deployed to secure HTTPS traffic. ICA connections are not allowed.
CSG3221	Client IP [*IP address*] attempted an HTTPS connection, current gateway installation mode does not allow HTTPS connections.	The Secure Gateway is deployed to secure ICA traffic. HTTPS connections are not allowed.
CSG3222	Client IP [*IP address*] sent unrecognized data at start of the connection, connection dropped.	The service refused the connection because connection data did not contain a supported protocol header.

Error Number	Error Message	Description
CSG3223	Authentication Service [*ID*] returned SOAP error [*error message text*] in response to validation request for client IP [*IP address*], connection dropped.	The server running the Authentication Service responded with an error. Ensure that the Authentication Service is installed and running on the specified server(s).
CSG3224	Authentication Service [*ID*] returned invalid SOAP packet in response to validation request for client IP [*IP address*], connection dropped.	The server running the Authentication Service responded with an error. Ensure that the Authentication Service is installed and running on the specified server(s).
CSG3225	Authentication Service [*ID*] failed to return a table ID in response to validation request for client IP [*IP address*], connection dropped.	The server running the Authentication Service responded with an error. Ensure that the Authentication Service is installed and running on the specified server(s).
CSG3226	Authentication Service [*ID*] returned an empty table [*table ID*] in response to validation request for client IP [*IP address*], connection dropped.	The server running the Authentication Service returned an empty table of accessible resources. Ensure that the Authentication Service is configured to publish resources.
CSG3227	Authentication Service [*ID*] failed to return a portal address in response to validation request for client IP [*IP address*], connection dropped.	The server running the Authentication Service failed to return the address of the access center specified by the access token from the client.
CSG3228	Client IP [*IP address*] sent invalid data as an SSL or TLS handshake, connection dropped.	The SSL handshake between this client IP address and the service failed. Possible causes are that the server certificate was not accepted by the client, encryption level mismatch, or network errors that prevented the client from completing the handshake before the connection time-out limit.
CSG3229	Client IP [*IP address*] sent unresolvable STA or Authentication Service, connection dropped.	The service is not configured to support the ID specified by the access token from the client. Reconfigure the Secure Gateway.
CSG3230	Client IP [*IP address*] connection dropped due to SChannel error specified by [*hex value*].	An internal error is returned by SChannel on the server running the Secure Gateway. Contact your Help Desk administrator for support.

Informational Messages

These messages are logged as a result of client connection events.

Error Number	Error Messages	Description
CSG4200	Information undefined.	Message is reserved for system use.
CSG4201	Client IP [*address*] with username [*username*] connected successfully to server [*FQDN*], using protocol [*protocol name*].	The service established the connection successfully.
CSG4202	Client IP [*address*] with username [*username*] successfully closed connection to server [*FQDN*], using protocol [*protocol name*].	The service closed the connection at the request of the client.
CSG4203	Server [*address*] successfully closed connection from client IP [*address*] with username [*username*], using protocol [*protocol name*].	The service closed the connection at the request of the server in the enterprise network.
CSG4204	STA or Authentication Service [*IP address*] closed socket. Attempting to reconnect.	The authority server closed the connection. The Secure Gateway is attempting to reconnect.
CSG4205	Request STA or Authentication Service [*ID*] to resolve ticket [*token value*].	The service requested the authority server to resolve the session ticket or the access token.

Logon Agent Messages

End User Specific Messages

The Logon Agent is responsible for presenting a logon interface when a user attempts to log on to the Secure Gateway. Users may encounter the following error messages related to the Logon Agent when attempting to log on.

Error Message	Description
Username must not be blank.	This error appears on the client browser. It indicates that the username field is left blank. Enter a username and try again.
Access denied.	This error appears on the client browser. It indicates that the authentication attempt failed. The Logon Agent reported an error authenticating the user. Check the credentials and try again.
RSA SecurID PASSCODE must not be blank.	This error appears on the client browser. It indicates that the RSA SecurID PASSCODE field is left blank. Enter the RSA SecurID PASSCODE and try again.

Messages Logged to the Internet Information Services (IIS) Log

System events and error messages for the Logon Agent are logged to the standard Internet Information Services (IIS) log files.

Check the IIS log file, %systemroot%\system32\LogFiles\W3SVC1*date*.log, for errors and events related to the Logon Agent.

Error Message	Description
File not found.	This error is logged to the IIS log file. It indicates that a file required to run the Logon Agent is missing. Your Logon Agent installation appears to be corrupted. Uninstall and reinstall the Logon Agent software.
Failed to initialize RSA SecurID interface (2000).	This error is logged to the IIS log file. It indicates that an error occurred during RSA SecurID authentication. Check that the RSA SecurID components and the authentication process are functioning correctly.
Internal error (2001).	This error is logged to the IIS log file. It indicates that an error occurred during RSA SecurID authentication. Check that the RSA SecurID components and the authentication process are functioning correctly.

The IIS log file tends to be verbose because each HTML request is logged. To identify messages related to the Logon Agent, find URLs related to the Logon Agent. A section of an IIS log file is shown below:

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-02-19 00:24:33
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)
2003-02-19 00:24:33 127.0.0.1 - 127.0.0.1 80 GET /index.htm - 404 -
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2003-02-19 00:40:23
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)

2003-02-19 23:46:25 127.0.0.1 - 127.0.0.1 80 GET /LogonAgent/themes/default/images/windowBackground.gif - 304 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)

2003-02-19 23:46:25 127.0.0.1 - 127.0.0.1 80 GET /LogonAgent/themes/default/images/logo.gif - 304 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)

2003-02-19 23:46:25 127.0.0.1 - 127.0.0.1 80 GET /LogonAgent/themes/default/images/background.gif - 304 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)

2003-02-19 23:46:28 127.0.0.1 - 127.0.0.1 80 POST /LogonAgent/Login.asp AS:domain/username;AS:Authenticate.xml+file+not+found; 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1)
```

The POST request, highlighted above, demonstrates a "*File not found*" error, which indicates that a file required to run the Logon Agent is missing.

For information about IIS log files and formats, refer to the IIS documentation.

STA Messages

The STA is designed to log fatal errors to its application log, sta*yyyymmdd-xxx*.log, located in the \inetpub\scripts directory. This file is created the first time the STA is loaded.

To view STA error messages, open the sta*yyyymmdd-xxx*.log file using a text editor such as Notepad.

Important Due to lack of write privileges to the \inetpub\scripts directory, the STA may not be successful in creating a log file. For instructions about enabling logging on the STA, see "Application Log for the STA Is Empty or Missing" on page 152.

Fatal Error Messages

The following messages are logged when a fatal error occurs. In all these cases, the STA cannot be started and ticketing fails. The best way to correct such problems is to reinstall the STA.

Error Number	Error Messages	Description
CSG1001	Unable to read config file.	The configuration file is missing or cannot be found.
CSG1002	Unable to initialize Random Generator.	The random generator is corrupted. The random generator is used to generate random number sequences that are used to encrypt tickets. If this component is not found or is malfunctioning, ticketing fails.
CSG1003	Unable to access XML translation file CtxXmlss.txt.	The CtxXmlss.txt file is the XML translation file used by the STA to translate input to UNICODE.
CSG1004	Insufficient memory to initialize system.	The system is unable to allocate memory required for the application. This error could occur if the system is running low on memory. Close some applications before trying again.
CSG1005	Missing entry in config file for *configuration parameter.*	*Configuration parameter* is not defined in the STA configuration file.

Application Error Messages

The following messages are logged as a result of the STA experiencing operational problems. The STA was started, but certain operations, such as generating performance data, fail.

Error Number	Error Message	Description
CSG1101	Unable to initialize performance counters.	The service cannot access memory for performance counters. Performance counter data is not updated.
CSG1102	No Ticket Store in memory.	Memory is not initialized at startup.
CSG1103	Unable to delete old log file.	The STA is unable to delete the oldest log file. The system attempts to delete the oldest log file when the number of log files reaches the maximum limit. This error could occur if the file is in use or its file attributes are changed.

Warning Messages

These messages are logged as a result of events caused by corrupted data requests or data packets received, ticket time-outs, and so on. In general, these errors are likely to occur when the data request originates from an unknown source.

Error Number	Error Message	Description
CSG1201	Request Data - Parsing failed, bad XML.	Data request packet contains bad XML data and cannot be parsed.
CSG1202	Request Data - No ticket or wrong ticket version in XML.	The request is not in the right format for the STA to resolve the ticket to its associated data. The request is rejected.
CSG1203	Request Data - Ticket not found.	The ticket requested is not found. This can occur if the ticket times out.
CSG1204	Request Ticket - Parsing failed, bad XML.	The ticket request failed because the STA encountered unknown XML data. The ticket cannot be parsed.
CSG1205	Request Ticket - No data or wrong type in XML.	Data request packet received contains no data or incorrect XML data. Ticketing failed.
CSG1206	Request Ticket - No memory to save data.	The system is low on memory and cannot save the ticket request.

Error Number	Error Message	Description
CSG1207	Request Ticket - Maximum reached, data NOT saved.	The maximum active ticket limit is reached. Ticketing failed. Increase the maximum ticket limit or reduce the ticket lifetime.
CSG1208	Request Ticket - Failed, data NOT saved.	A system error occurred when trying to save this ticket.
CSG1209	Unused tickets still in IMDB at unload.	The STA terminated abruptly. Unused tickets are still present in the In-Memory Database (IMDB).

Informational Messages

These information messages are logged as a result of normal STA operations.

Error Number	Error Message	Description
CSG1301	CtxSTA.dll Loaded.	The STA is started.
CSG1302	CtxSTA.dll Unloaded.	The STA is unloaded (stopped).
CSG1303	Ticket Timed Out.	This ticket reached the maximum ticket lifetime and has now expired.
CSG1304	Request Data - Successful.	This ticket data request is successful.
CSG1305	Request Ticket - Successful.	This ticket request is successful.
CSG1306	Log file index reset to 000 (from 999).	1000 log files were generated in a 24-hr. period. The STA now reuses the oldest log file, *STAyyyymmdd*-000.log.

Go to Document Center

APPENDIX C

Glossary

This appendix provides a glossary of terms and acronyms used throughout the Secure Gateway documentation.

access center A Web site that aggregates information and services for a community of users inside or outside an organization.

access server farm One or more networked computers that run MetaFrame Secure Access Manager components and work together to host MetaFrame Secure Access Manager access centers. Each access server farm includes a Web server, SQL database server, state server, and agent server.

access control list (ACL) In the context of the Secure Gateway, an access control list (ACL) is a mechanism that restricts access to resources. The ACL is a data structure containing the IP addresses and ports of computers running MetaFrame Presentation Server on the network to which Secure Gateway components have access.

authentication The process of identifying an individual, usually based on a user name and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Authentication Service A service available on a server running MetaFrame Secure Access Manager that issues access tokens for HTTP connection requests for resources available from an access center. These access tokens form the basis of authentication and authorization for HTTP/S connections to an access center.

authorization The process of granting or denying access to a network resource. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who they claim to be. The second stage is authorization, which allows the user access to various resources based on the user's identity.

certificate An attachment to electronic data used for security purposes. The most common use of a digital certificate is to verify that a user sending the data is who they claim to be, and to provide the receiver with the means to encode a reply.

ciphersuites An encryption/decryption algorithm. When establishing an SSL/TLS connection, the client and server determine a common set of supported *ciphersuites* and then use the most secure one to encrypt the communications. These algorithms have differing advantages in terms of speed, encryption strength, exportability, and so on.

Citrix XML Service A Windows NT service that provides an HTTP interface to the client's browser. It uses TCP packets instead of UDP, which allows connections to work across most firewalls. The default port for the Citrix XML Service is 80.

demilitarized zone (DMZ) A network isolated from the trusted or secure network by a firewall. Network administrators often isolate public resources, such as Web or email servers in the DMZ to prevent an intruder from attacking the internal network.

Gateway Client An ActiveX control, available on a server running MetaFrame Secure Access Manager, that downloads automatically to an authenticated, remote client browser when the user connects to an access center and attempts to access resources hosted on internal Web servers. The Gateway Client functions as a proxy between the client device and the Secure Gateway.

ICA Independent Computing Architecture. The architecture that MetaFrame Presentation Server uses to separate an application's logic from its user interface. With ICA, only the keystrokes, mouse clicks, and screen updates pass between the client and server on the network, while 100% of the application's logic executes on the server.

ICA file (.ica) A text file (with the extension ica) containing information about a published application. ICA files are written in Windows Ini file format and organize published application information in a standard way that MetaFrame Presentation Server Clients can interpret. When a client receives an ICA file, it initializes a session running the specified application on the server specified in the file.

ICA protocol The protocol that MetaFrame Presentation Server Clients use to format user input (keystrokes, mouse clicks, and so forth) and address it to servers for processing. Servers use the ICA protocol to format application output (display, audio, and so forth) and return it to the client device.

ICA session A lasting connection between a client and a computer running MetaFrame Presentation Server, identified by a specific user ID and ICA connection. It consists of the status of the connection, the server resources allocated to the user for the duration of the session, and any applications executing during the session. An ICA session normally terminates when the user logs off from the server.

Logon Agent A component of the Secure Gateway that provides the logon interface when users log on to Secure Gateway. The Logon Agent is responsible for facilitating the authentication of user credentials entered by a user attempting to connect to MetaFrame Secure Access Manager.

MetaFrame Presentation Server Client Citrix software that enables users to connect to computers running MetaFrame Presentation Server from a variety of client devices.

MetaFrame Presentation Server Server on which MetaFrame Presentation software is running. You can publish applications, content, and desktops for remote access by clients on these servers.

NFuse Classic See Web Interface for MetaFrame.

Program Neighborhood The user interface for the MetaFrame Presentation Server Client for 32-bit Windows and MetaFrame Presentation Server Client for Java, that lets users view the published resources they are authorized to use in the server farm. Program Neighborhood contains application sets and custom ICA connections.

published application An application installed on a computer running MetaFrame Presentation Server or server farm that is configured for multiuser access from clients. With Load Manager, you can manage the load for published applications among servers in the server farm. With Program Neighborhood and the Web Interface, you can push a published application to your users' client devices.

relay mode Not available with the Secure Gateway. Deprecated mode of use available in Citrix Secure Gateway, Version 1.x. In this mode, the Secure Gateway functions without ticketing support from the STA and the Web Interface. It is a less secure mode, in which the Secure Gateway functions as a server-side proxy server and provides a single point of entry into a server farm.

Secure Gateway A MetaFrame that provides a secure, encrypted channel for HTTP and ICA traffic over the Internet, using SSL (Secure Sockets Layer) or TLS (Transport Layer Security) between client devices and the Secure Gateway. The Secure Gateway provides a single point of encryption and access to servers running MetaFrame Presentation Server and MetaFrame Secure Access Manager.

Secure Gateway Proxy A component of the Secure Gateway that functions as a proxy server between the Secure Gateway and the secure network.

Secure Ticket Authority (STA) The STA is a ticketing mechanism that issues session tickets for clients. These tickets form the basis of authentication and authorization for connections to a server farm.

server farm A group of computers running MetaFrame Presentation Server managed as a single entity (or system image) with some form of physical connection between the member servers and an IMA-based data store, thus providing centralized administration and horizontal scalability.

session ID A unique identifier for a specific client session on a specific computer running MetaFrame Presentation Server.

Web Interface A component that works with MetaFrame Presentation Server to deliver server-based applications through Web pages.

Index

A

accelerators cards, SSL 139
access center 17, 28–29
access control list (ACL) 38
Acrobat Reader, requirements 11
authentication 22, 159, 187
Authentication Service 16
authorization 22, 187

C

CAs. See certificate authorities
certificate authorities 158–159
certificates 155, 158, 188
  certificate chains 160
  chain 160
  content 159
  creating a certificate request 163
  CRLs 161
  double-hop DMZ 47
  expiration 161
  hierarchy 160
  obtaining 162
  private CA 162
  public CA 162
  renewal 161
  request, creating 163
  response file 164
  single-hop DMZ 44
  trial period 163
  verification process 162
  where to get them 162
chain certificates 160
cipher 156
ciphersuites 142–143, 188
  COM 142
  GOV 142
Citrix XML Service 16, 19, 188
COM 142
communications links, securing 21
compatibility
  client devices 42
  MetaFrame Presentation Server 43
  NFuse Classic 43
  Web Interface 43
configuration values, requiring restart 119
connection keep-alive settings 139–140
context-sensitive help 51
cryptography 156–157
  asymmetric encryption 157
  public key 157
  secret key 157
  symmetric key 157
customizing 404 error handler 63

D

default Web page 62
demilitarized zone 14, 142
deployment
  configuration options 56
  MetaFrame Secure Access Manager, including 55
  SecurID integration 67
  topologies, recommended 88
diagnostic tools 21, 126, 148
Digital certificates. See certificates
DMZ. See demilitarized zone
documentation, additional 9
double-hop DMZ 37, 75, 98
downloading, Gateway Client 131

E

error messages 171
  viewing 172
exporting server certificates 166

F

fatal error messages 174
fault tolerance 23, 137
FIPS 140 156

firewalls
forwarding mode 136
ICA traffic, supporting 136
proxy mode 136
traversal 23, 136

G

Gateway Client 16, 42, 130
connection details 133
device compatibility 42
downloading 131
icon 132
installation path 131
Glossary 187
GOV 142

H

hardware requirements 40
hash function 157
high availability 137
HTTP 404 errors 63
HTTPS 21

I

ICA
file 188
protocol 188
session 188
IETF 156
IIS log file 181
importing, X.509 certificate 165
information messages 180
installation
cancelling 51
configuration wizards 51
pre-installation tasks 48
procedure 50
removing components 53
selecting components 51
sequence 48
server certificates 163
upgrading components 52
intermediate CAs 160
internal Web servers 16
Internet Explorer
compatibility 43
high encryption pack 43
Internet security protocols 156
ISO X.509 protocol 158

K

keep-alive parameters 139–140
registry keys 141

L

load balancing 135, 137–138
benefits 138
certificate requirements 138
Secure Gateway array 135, 138
SSL accelerator cards 139
STA, servers running 139
logging 23
Logon Agent 16
messages 181
requirements 41

M

management and report tools 21

N

NFuse Classic 19, 189

O

outbound restrictions 64

P

performance monitoring 120
PKCS #12 163
PKI 156
private CA 162
Program Neighborhood 189
public CA 162
published application 189

R

redirecting HTTP 404 errors 63
redundancy 137
relay mode 52, 189
restricting 143
revocation lists 161
root certificate 159, 169
installing 169
obtaining 169

RSA ACE Agent 41
test authentication 70
RSA ACE/Server 68
RSA SecurID integration 22

S

Secure Gateway Proxy
load balancing 138
requirements 40
Secure Sockets Layer. See SSL
Secure Ticket Authority 16, 19, 189
application errors 183
fatal error messages 183
high availability 139
informational messages 185
installation path, default 64
minimum requirements 41
multiple servers running the STA, deploying 139
unique ID 64
warning messages 184
SecurID token 69
security concepts 155
security recommendations 142
server certificate 159
applying for 164
certificate request, creating 163
installing 163
server farm 17, 20, 31, 189
connecting to 28
connection process 31
defined 189
session ID 190
single-hop DMZ 56, 58
software requirements 40
SSL 144, 156
accelerator cards 139
status messages 173
subordinate CAs 160

T

TCP/IP keep-alives 140
test certificates 163
TLS 144, 156
Transport Layer Security. See TLS

U

uninstalling 53
upgrading components 52

V

VPN 22

W

warning messages 177
Web Interface 19
firewall settings 89
limitations 88
proxy settings 89
Website Viewer CDA 69
Windows registry
keep-alive parameters 141

X

X.509 format file 163, 165

Z

.cer 163
.ica 188
.pfx 163