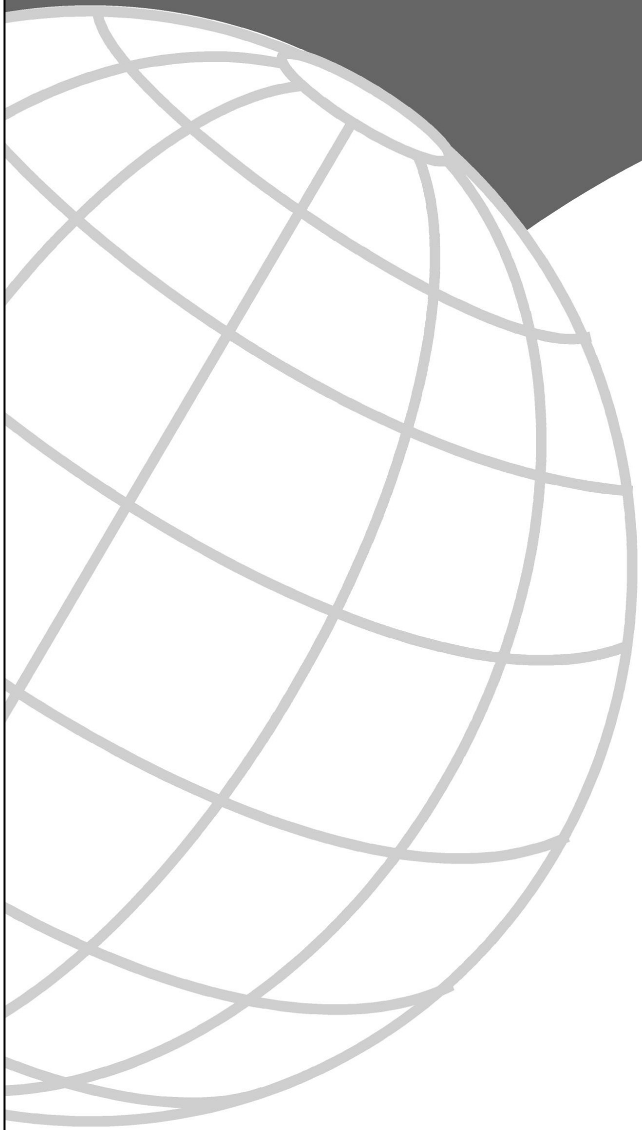


Enabling Service Excellence

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows 2008, Windows 2012, Windows 2016, Windows 7, Windows 8 and Windows 2010 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

Table of contents

Table of Figures

1

Administering the eG Manager to work with a Citrix Secure Gateway

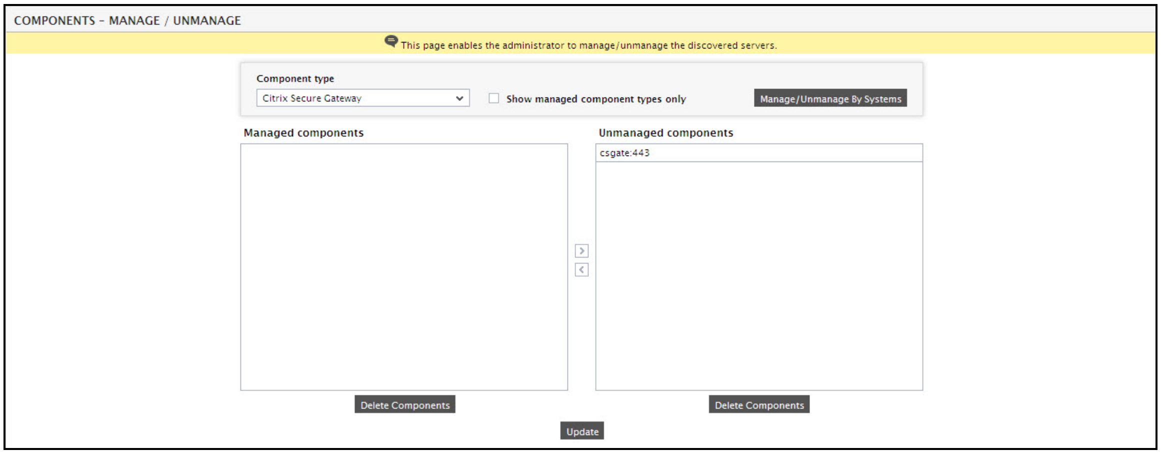
To do the above, do the following:

1. Log into the eG administrative interface.

2. If a Citrix Secure Gateway is already discovered, then directly proceed towards managing it using the **COMPONENTS - MANAGE/UNMANAGE** page (Infrastructure -> Components -> Manage/Unmanage). However, if it is yet to be discovered, then run discovery (Infrastructure-> Components -> Discover) to get it discovered or add the Citrix Secure Gateway manually using the **COMPONENTS** page (Infrastructure-> Components -> Add/Modify). Remember that components manually added are managed automatically. Discovered components, however, are managed using the **COMPONENTS - MANAGE/UNMANAGE** page. Figure 1.1 and Figure 1.2 clearly illustrate the process of managing a Citrix Secure Gateway.

   Reference :

   For more details on managing components, refer to *Configuring and Monitoring Web Servers* document.



COMPONENTS - MANAGE / UNMANAGE

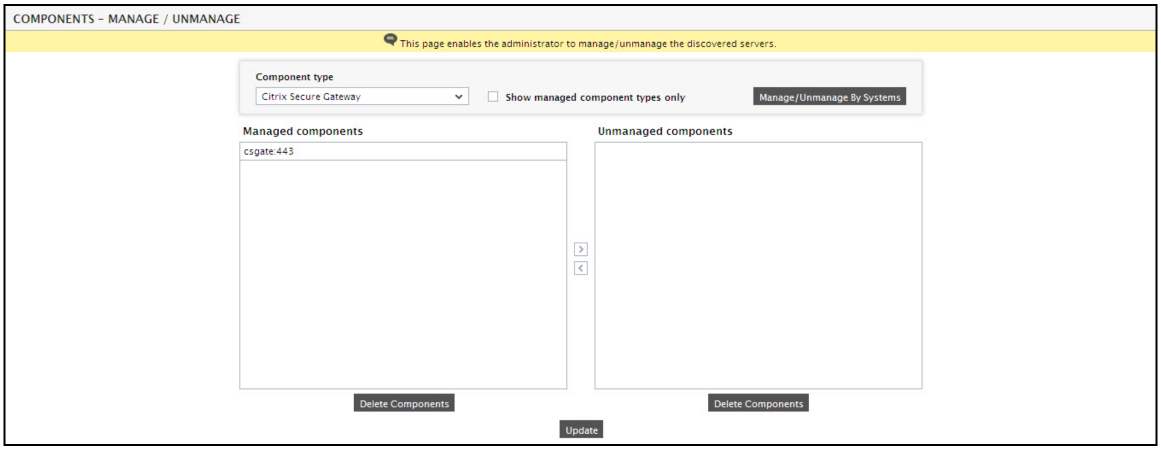
This page enables the administrator to manage/unmanage the discovered servers.

Component type: Citrix Secure Gateway

□ Show managed component types only

Unmanaged components: csgate:443

Figure 1.1: Selecting the Citrix Secure Gateway to be managed



COMPONENTS - MANAGE / UNMANAGE

This page enables the administrator to manage/unmanage the discovered servers.

Component type: Citrix Secure Gateway

□ Show managed component types only

Managed components: csgate:443

Unmanaged components:

Figure 1.2: Managing the Citrix Secure Gateway server

3. Next, sign out of the eG administrative interface.

2

Monitoring Citrix Secure Gateway

Citrix Secure Gateway of the Citrix Access Suite is a Citrix infrastructure component which can be used to secure access to resources and applications hosted on servers running one or more Citrix server products. The Secure Gateway transparently encrypts and authenticates all user connections to protect against data tampering and theft.

In order to maintain data integrity and safety, it is imperative to ensure the uninterrupted functioning of the Citrix Secure Gateway. eG Enterprise's specialized monitoring model for the *Citrix Secure Gateway* keeps close tabs on every critical step of the authentication operation performed by the Secure Gateway server, so that potential security breaches are spotted and sealed before they disrupt normal server functions; this includes, the identification of connection bottlenecks, monitoring data transmitted to and from the server to detect a possible overload, assessing how effectively the server handles SSL handshakes, determining whether/not the server properly validates login credentials, etc.

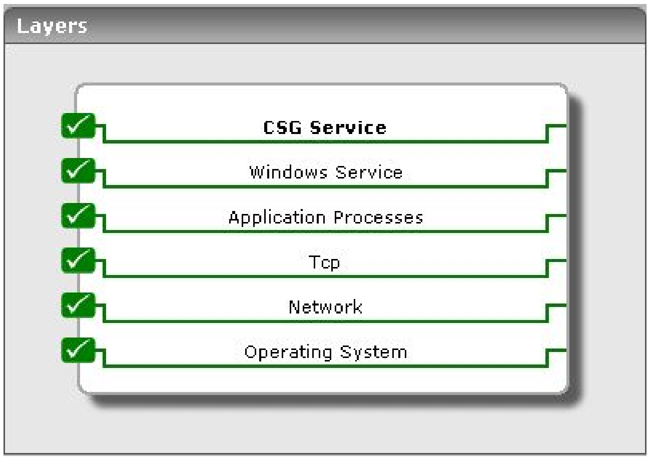


Figure 2.1: The layer model of a Citrix secure gateway server

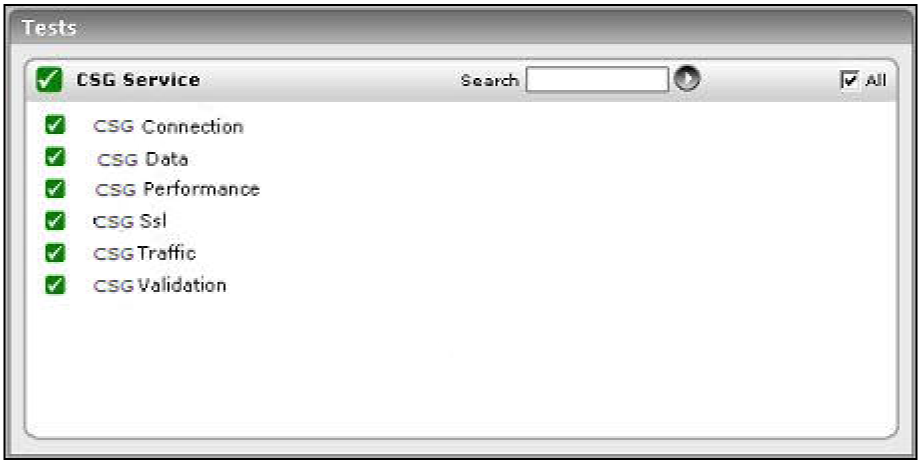
The tests mapped to each of the layers present in Figure 2.1 aid in the monitoring of one or more of the aforesaid performance parameters. As the lower 5 layers of the layer model have been dealt with extensively in the *Monitoring Unix and Windows Servers* document, this section will discuss the **CSG Service** layer only.

2.1 The CSG Service Layer

Using the tests associated with this layer, you can monitor:

- Connection attempts made to the server and their success and failure rates
- Data sent to and received by the server

- The status of validations performed
- SSL handshakes



Tests

☑ CSG Service Search ☑ All

☑ CSG Connection
☑ CSG Data
☑ CSG Performance
☑ CSG Ssl
☑ CSG Traffic
☑ CSG Validation

Figure 2.2: The tests associated with the CSG Service layer

2.1.1 CSG Connection Test

This test reports statistics related to the connections established between the ICA client and the Citrix Secure Gateway Server.

Target of the test : Any Citrix Secure Gateway server

Agent deploying the test : An external agent

Outputs of the test : One set of results is reported for every Citrix secure gateway server being monitored

Configurable parameters for the test:

1. **TEST PERIOD** – How often should the test be executed
2. **HOST** – The host for which the test is to be configured
3. **PORT** – Refers to the port used by the Citrix secure gateway server
4. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.

   The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

   - The eG manager license should allow the detailed diagnosis capability
   - Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active HTTP connections:	The total number of HTTP/HTTPS client sessions currently active through Secure Gateway.	Number	This measure is incremented for each successful client connection request and is decremented for each disconnected or terminated HTTP/S connection.
Active ICA connections:	The total number of ICA Client sessions currently active through the Secure Gateway Service.	Number	The measure is incremented for each successful ICA Client connection request and decremented for each disconnected or terminated ICA connection.
Active other connections:	These are connections to the Logon Agent or the Web Interface to MetaFrame XP. This measure indicates the total number of client sessions currently active through the Secure Gateway Service that are not yet authenticated.	Number	The measure is incremented for each successful client connection request and is decremented for each disconnected or terminated non-ICA or HTTP/S connection.
Pending connections:	The total number of client connection requests that were accepted but have not yet completed the connection process.	Number	The measure is incremented when a client connection request is accepted and is decremented when the client connection request succeeds or fails.
Percentfailed connections:	Percentage of failed connections.	Percent	
Failed connections:	The total number of failed client connection requests.	Number	The measure is incremented when a client fails to complete the handshaking process or a connection could not be established to the requested resource. The constant increase in failed

Measurement	Description	Measurement Unit	Interpretation
			connections, interprets failure due to various factors like Timed Out, SSL error, Server Connect error, Authentication error and Access control list errors. The detailed diagnosis capability of this measure, if enabled, provides the number of connections which failed due to each of the above-mentioned reasons.

2.1.2 CSG Traffic Test

This test reports the statistics pertaining to the to and fro data traffic between the ICA Client and the Citrix Secure Gateway after the connection has been established.

Target of the test : Any Citrix Secure Gateway server

Agent deploying the test : An internal agent

Outputs of the test : One set of results is reported for every Citrix secure gateway server being monitored

Configurable parameters for the test

1. **TEST PERIOD** – How often should the test be executed
2. **HOST** – The host for which the test is to be configured
3. **PORT** – Refers to the port used by the Citrix secure gateway server

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data receive rate:	The total number of bytes (for all client connections) sent to the Secure Gateway Service by any connected client.	KB/Sec	The measure is increased when the Secure Gateway Service reads some data from a connected client.
Data send rate:	The total number of bytes	KB/Sec	The measure is increased when the

Measurement	Description	Measurement Unit	Interpretation
	(for all client connections) sent to the client(s) from the Secure Gateway Service.		Secure Gateway Service sends data to any connected client.

2.1.3 CSG Validation Test

This test reports results of the validations done by the Secure Ticket Authority before getting access to the Citrix Gateway Server.

Target of the test : Any Citrix Secure Gateway server

Agent deploying the test : An internal agent

Outputs of the test : One set of results is reported for every Citrix secure gateway server being monitored

Configurable parameters for the test

1. **TEST PERIOD** – How often should the test be executed
2. **HOST** – The host for which the test is to be configured
3. **PORT** – Refers to the port used by the Citrix secure gateway server

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Failed ticket validations:	The rate of unsuccessful STA ticket validation requests.	Validations/Sec	If a ticket is not validated by the STA or the Secure Gateway Service, the measure is increased. More than 5 ticket validations indicate that the client configuration in the Metaframe should be investigated.
Failed access token validations:	The total number of unsuccessful access token validations.	Errors/Sec	This counter is incremented if an access token cannot be validated by the Authentication Service or there is an error while the Secure Gateway Service is attempting to validate the access token. More than 3 validation errors

Measurement	Description	Measurement Unit	Interpretation
			interprets that the state of the tickets generated should be verified or the connation between the Client and SecureGateway should be checked.
Successful validations:	The rate of validations succeeded	Validations/Sec	
Successful cache validations:	The rate at which successful access token validations occur in the Secure Gateway Service matching the contents of its cache.	Validations/Sec	The measure is increased when the Secure Gateway Service successfully validates an access token by checking if it has the access token in its cache.
Successful STA validations:	The rate at which successful validations occur through Authentication Service in response to access token validation requests from the Secure Gateway Service.	Validations/Sec	The measure is increased when the Authentication Service returns a validation successful message.

2.1.4 CSG SSL Test

This test monitors the SSL handshakes handled by a Citrix Secure Gateway.

Target of the test : Any Citrix Secure Gateway server

Agent deploying the test : An internal agent

Outputs of the test : One set of results is reported for every Citrix secure gateway server being monitored

Configurable parameters for the test

1. **TEST PERIOD** – How often should the test be executed
2. **HOST** – The host for which the test is to be configured
3. **PORT** – Refers to the port used by the Citrix secure gateway server

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
SSL Handshakes:	The number of SSL handshakes handled by the CSG in the last measurement period.	Number	
SSL handshake rate:	The rate at which SSL handshakes are being handled by the CSG.	Handshakes/Sec	This value is one of the representations of the workload on the CSG.
Pending SSL handshakes:	The number of SSL handshakes currently in progress between the CSG and clients.	Number	Ideally, this value should be low.
Avg SSL handshake time:	The average time taken for an SSL handshake to complete.	Secs	This value indicates whether SSL handshakes are slowing down user access to the Citrix infrastructure.

2.1.5 CSG Data Test

This test monitors the data to and from the Citrix Secure Gateway to clients. Protocol-wise breakup of the data communicated is also provided.

Target of the test : Any Citrix Secure Gateway server

Agent deploying the test : An internal agent

Outputs of the test : One set of results is reported for every Citrix secure gateway server being monitored

Configurable parameters for the test

1. **TEST PERIOD** – How often should the test be executed
2. **HOST** – The host for which the test is to be configured
3. **PORT** – Refers to the port used by the Citrix secure gateway server

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Traffic rate to clients:	The rate of data transmitted to clients by the CSG.	KB/Sec	This value represents the workload on the CSG.
CGP data rate to clients:	The rate of CGP protocol data transmitted by the CSG to clients.	KB/Sec	
SOCKS traffic to clients:	The rate of SOCKS protocol data transmitted by the CSG to clients.	KB/Sec	
HTTP traffic to clients:	The rate of HTTP/HTTPS protocol data transmitted by the CSG to clients.	KB/Sec	
Data traffic from clients:	The rate of data transmitted from clients by the CSG.	KB/Sec	This value represents the workload from the CSG.
CGP data from clients:	The rate of CGP protocol data transmitted from the CSG to clients.	KB/Sec	
SOCKS traffic from clients:	The rate of SOCKS protocol data transmitted from the CSG to clients.	KB/Sec	
HTTP traffic from clients:	The rate of HTTP/HTTPS protocol data transmitted from the CSG to clients.	KB/Sec	

2.1.6 CSG Performance Test

This test monitors connections to the Citrix Secure Gateway.

Target of the test : Any Citrix Secure Gateway server

Agent deploying the test : An internal agent

Outputs of the test : One set of results is reported for every Citrix secure gateway server being monitored

Configurable parameters for the test

1. **TEST PERIOD** – How often should the test be executed
2. **HOST** – The host for which the test is to be configured
3. **PORT** – Refers to the port used by the Citrix secure gateway server

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Successful connections to the CSG:	The number of successful connections handled by the Citrix Secure Gateway during the last measurement period.	Number	
Successful CGP connections:	The number of successful CSG protocol connections handled by the Citrix Secure Gateway during the last measurement period.	Number	
Successful SOCKS connections:	The number of successful SOCKS protocol connections handled by the Citrix Secure Gateway during the last measurement period.	Number	
Successful HTTP connections:	The number of successful HTTP/HTTPS protocol connections handled by the Citrix Secure Gateway during the last measurement period.	Number	
Current active connections to the CSG:	The number of connections currently being handled by the CSG.	Number	If the number of active connections is unusually high or low, it may indicate a situation that warrants further investigation to see if the Citrix infrastructure is working well.
Active CGP	The number of CGP	Number	

Measurement	Description	Measurement Unit	Interpretation
connections:	connections currently being handled by the CSG.		
Active Socks connections to the CSG:	The number of SOCKS connections currently being handled by the CSG.	Number	
Active HTTP connections to the CSG:	The number of HTTP/HTTPS connections currently being handled by the CSG.	Number	
Failed connections to the CSG:	The total number of failed client connection requests during the last measurement period.	Number	This value is the sum of the Failed Connections (Timed Out), Failed Connections (SSL Error), and Failed Connections (General Client Error) counters.
Percent failed connections:	The percentage of total connections handled that failed.	Percent	
Client timeouts:	The total number of client connection requests that were accepted but timed out before completing the protocol handshake during the last measurement period.	Number	
SSL handshake errors:	The total number of client connection requests that were accepted but did not successfully complete the SSL handshake during the last measurement period.	Number	
Client errors:	The total number of client connection requests that	Number	

Measurement	Description	Measurement Unit	Interpretation
	failed to connect to the Secure Gateway for any reason other than timing out or SSL handshake error during the last measurement period.		
Avg client connection time:	The average amount of time (in Secs) for a client connection request to complete the connection process.	Secs	
Failed backend connections:	The total number of backend connections that failed in the last measurement period.	Number	Clients that successfully connect to the Secure Gateway may not successfully connect to backend servers, such as a Web server. These connections are not counted as part of the failed client connection count.
Pending connections:	The total number of client connection requests accepted, but not yet completed by the Secure Gateway.	Number	Pending connections are still active and have not timed out or failed. An increase in pending connections indicates a potential bottleneck at the CSG.

3

Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to **Citrix Secure Gateway**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.