



Monitoring Citrix Federated Authentication Server (CFAS)

eG Innovations Product Documentation

www.eginnovations.com



Table of Contents

CHAPTER 1: INTRODUCTION TO MONITORING CITRIX FEDERATED AUTHENTICATION SERVER (CFAS)	1
1.1 How Does eG Enterprise Monitor the Citrix Federated Authentication Server?	2
CHAPTER 2: HOW TO MONITOR CITRIX FEDERATED AUTHENTICATION SERVER USING EG ENTERPRISE?	3
2.1 Managing the Citrix Federated Authentication Server	3
2.2 Configuring Tests for the Citrix Federated Authentication Server	4
CHAPTER 3: MONITORING THE CITRIX FEDERATED AUTHENTICATION SERVER	6
3.1 The Citrix Federated Authentication Service Layer	7
3.1.1 Citrix FAS Authorization Certificates Test	7
3.1.2 Citrix FAS Authorization Definitions Test	9
3.1.3 Citrix FAS Details Test	12
3.1.4 Citrix FAS MS Certificate Authority Details Test	14
3.1.5 Citrix FAS Servers Test	16
3.1.6 Citrix FAS User Certificate Details Test	18
ABOUT EG INNOVATIONS	20

Table of Figures

Figure 1.1: How CFAS integrates with Microsoft Certification Authority	1
Figure 2.1: Adding a Citrix Federated Authentication Server	4
Figure 2.2: List of unconfigured tests for CFAS	4
Figure 2.3: Configuring the Citrix FAS MS Certificate Authority Details test	5
Figure 3.1: Layer model of the Citrix Federated Authentication Server	6
Figure 3.2: The tests mapped to the Citrix Federated Authentication Service layer	7

Chapter 1: Introduction to Monitoring Citrix Federated Authentication Server (CFAS)

The Citrix Federated Authentication Service is a privileged component designed to integrate with Active Directory Certificate Services. It dynamically issues certificates for users, allowing them to log on to an Active Directory environment as if they had a smart card. This allows StoreFront to use a broader range of authentication options, such as SAML (Security Assertion Markup Language) assertions. SAML is commonly used as an alternative to traditional Windows user accounts on the Internet.

The following diagram shows the Federated Authentication Service integrating with a Microsoft Certification Authority and providing support services to StoreFront and XenApp and XenDesktop Virtual Delivery Agents (VDAs).

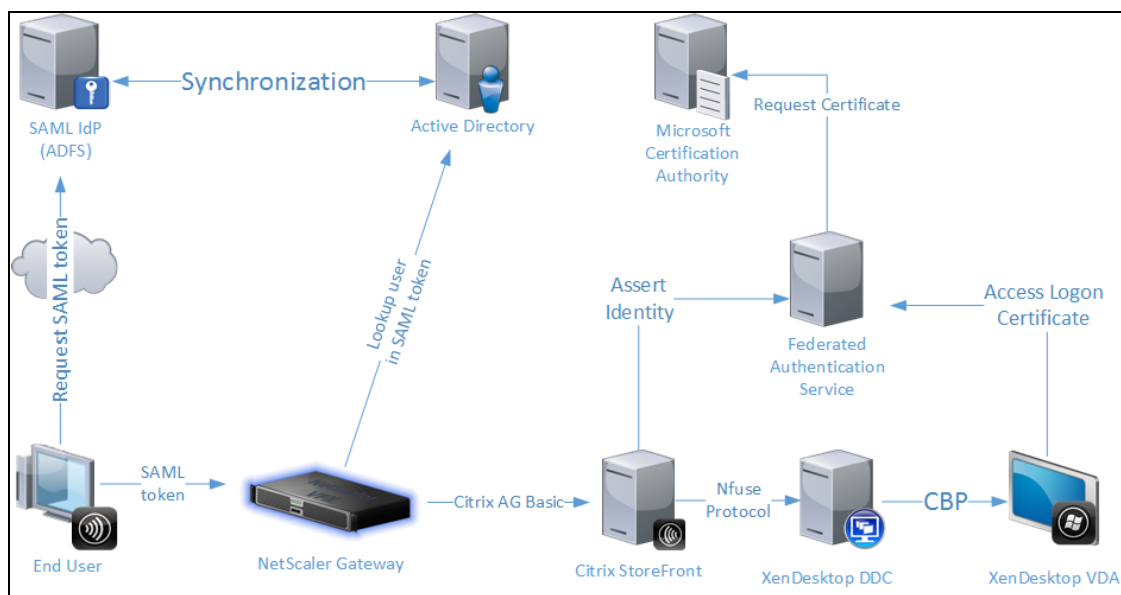


Figure 1.1: How CFAS integrates with Microsoft Certification Authority

Trusted StoreFront servers contact the Federated Authentication Service (FAS) as users request access to the Citrix environment. The FAS, in conjunction with Microsoft Certification Authority, grants a ticket that allows a single XenApp or XenDesktop session to authenticate with a certificate for that session. When a VDA needs to authenticate a user, it connects to the FAS and redeems the ticket. Only the FAS has access to the user certificate's private key; the VDA must send each signing and decryption operation that it needs to perform with the certificate to the FAS.

If the Certification Authority (CA) is inaccessible, then Citrix FAS will not be able to acquire the Authorization Certificate from the CA for issuing user certificates. This can result in user logon failures, which may cause users to be denied access to critical resources in the Citrix environment. Likewise, if Citrix FAS consistently takes too long to sign certificate requests, it is bound to delay user authentication; this can permanently damage user experience with Citrix. To avoid such unpleasant outcomes, administrators should closely track the availability of and the load on CFAS, the status of certificates it manages, and its interactions with the Certification Authorities, and proactively detect abnormalities. This is where eG Enterprise helps!

eG Enterprise supports monitoring of CFAS. With the help of eG Enterprise, you can continuously monitor the availability state and operational health of CFAS. You can thus keep an eye out for deviations in the status and operational health of the CFAS and be alerted to such deviations before end-users notice.

This document topic discusses how eG Enterprise monitors CFAS, how to manage CFAS using the eG web console, and what metrics eG reports for CFAS.

1.1 How Does eG Enterprise Monitor the Citrix Federated Authentication Server?

eG Enterprise monitors CFAS using an **agent-based** monitoring model. The eG agent installed on CFAS runs powershell scripts to pull metrics. Most of these scripts run out-of-the-box, and require no additional configuration.

To execute the **Citrix FAS Microsoft Certificate Authority Details** test alone, domain administrator privileges are required. Therefore, you need to configure this test with the valid **Domain** name of the CFAS, and the credentials of the domain administrator.

Chapter 2: How to Monitor Citrix Federated Authentication Server Using eG Enterprise?

Monitoring CFAS involves the following broad steps:

- Managing the CFAS
- Configuring tests for the CFAS

Each of these steps are discussed elaborately.

2.1 Managing the Citrix Federated Authentication Server

eG Enterprise does not automatically discover the Citrix Federated Authentication Server. Therefore, you will have to manually add the CFAS to the eG Enterprise system. The steps to achieve this are as follows:

1. Login to the eG admin interface.
2. Follow the Infrastructure -> Components -> Add/Modify menu sequence.
3. Figure 2.1 will then appear.

Category: All | Component type: Citrix Federated Authentication Server

Component information

Host IP/Name: 192.168.10.130

Nick name: cfas130

Port number: 432

Monitoring approach

Agentless: ☐

Internal agent assignment: ☒ Auto ☐ Manual

External agents: 192.168.8.110, dummyagent, mylogonsimagent, myVDIExtraRemoteagent

Add

Figure 2.1: Adding a Citrix Federated Authentication Server

4. In Figure 2.1, specify the **Host IP/Name** of the Citrix Federated Authentication Server to be monitored. Assign a unique **Nick name** to the server. Specify the **Port number** at which the server listens. Choose the **External agent** that will monitor the network availability and responsiveness of the target server.
5. Next, click the **Add** button to add the component.
6. Finally, click **Sign out** to exit the eG admin interface.

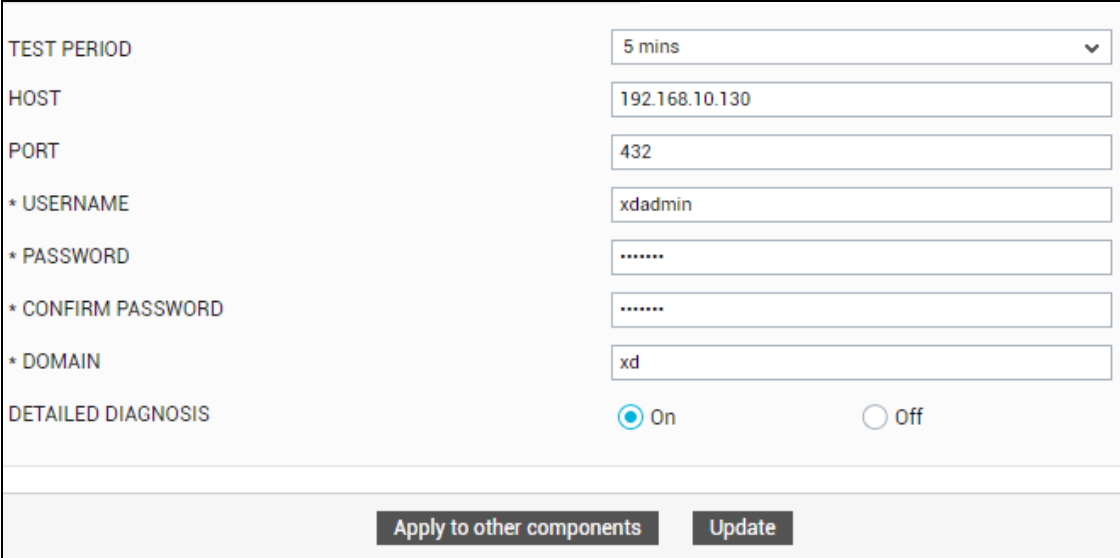
2.2 Configuring Tests for the Citrix Federated Authentication Server

When you attempt to sign out, you will be prompted to configure the **Citrix FAS MS Certificate Authority Details** test (see Figure 2.2). This test auto-discovers the Microsoft certificates managed by CFAS and reports whether/not each certificate is accessible.

LIST OF UNCONFIGURED TESTS FOR 'CITRIX FEDERATED AUTHENTICATION SERVER'		
PERFORMANCE		CFAS130:432
Citrix FAS MS Certificate Authority Details		

Figure 2.2: List of unconfigured tests for CFAS

To configure this test, click on it in Figure 2.2. Figure 2.3 will then appear.



The screenshot shows a configuration form for the Citrix FAS MS Certificate Authority Details test. The form has the following fields and controls:

- TEST PERIOD**: A dropdown menu set to "5 mins".
- HOST**: A text input field containing "192.168.10.130".
- PORT**: A text input field containing "432".
- * USERNAME**: A text input field containing "xdadmin".
- * PASSWORD**: A password input field with masked characters "*****".
- * CONFIRM PASSWORD**: A password input field with masked characters "*****".
- * DOMAIN**: A text input field containing "xd".
- DETAILED DIAGNOSIS**: A toggle switch currently set to "On" (indicated by a blue dot).
- At the bottom, there are two buttons: "Apply to other components" and "Update".

Figure 2.3: Configuring the Citrix FAS MS Certificate Authority Details test

To configure this test, specify the following parameters in Figure 2.3:

- **TEST PERIOD** - How frequently should the test execute.
- **HOST** - The host on which the test runs.
- **PORT** - The port number at which the HOST listens.
- **DOMAIN** - The name of the domain to which the target CFAS belongs.
- **USERNAME, PASSWORD, CONFIRM PASSWORD** - This test requires domain administrator privileges to run. Therefore, specify the credentials of such a user against **USERNAME** and **PASSWORD**. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box.
- **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.
- Finally, click the **Update** button to save the configuration.

Once the test is configured, log out of the eG web console.

Chapter 3: Monitoring the Citrix Federated Authentication Server

eG Enterprise provides a specialized monitoring model for the Citrix Federated Authentication Server.

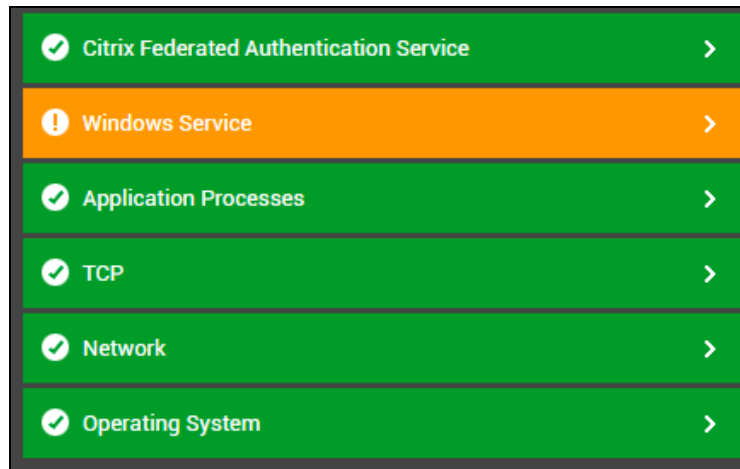


Figure 3.1: Layer model of the Citrix Federated Authentication Server

Each layer of this model is associated with tests that report on a wide variety of KPIs related to the CFAS. Using the metrics so reported, administrators can find quick and accurate answers for the following performance queries:

- Is the Citrix FAS server available over the network? If so, is it responding well to network requests?
- Has any authorization certificate expired?
- Can any user certificate be used as an in-session smart card?
- Has any user certificate expired? If so, which one?
- Is any Certificate Authority (CA) inaccessible?
- Is any FAS server in maintenance mode? If so, which one?
- How much time is the Citrix FAS server taking to process certificate signing requests? Is there a processing bottleneck on the server?
- How is the request load on the server - high? medium? or low?

Since the bottom five layers are already discussed in the Monitoring Unix and Windows Servers document, we will be taking only the **Citrix Federated Authentication Service** layer up for discussion.

3.1 The Citrix Federated Authentication Service Layer

Using the tests mapped to this layer, you can:

- Check whether/not the Certificate Authorities are accessible;
- Track the status of Authorization Certificates;
- View the definition of certificates
- Determine which servers are in the maintenance mode
- Know which user certificates have expired;
- Measure the request processing ability of the Citrix FAS server, and identify bottlenecks

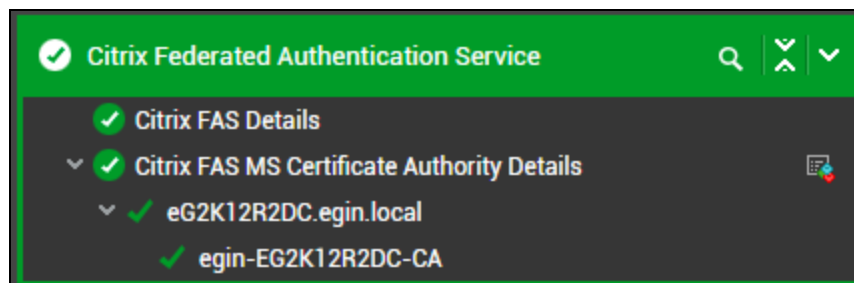


Figure 3.2: The tests mapped to the Citrix Federated Authentication Service layer

3.1.1 Citrix FAS Authorization Certificates Test

The Federated Authentication Service works by dynamically issuing user logon certificates from a Microsoft Certificate Authority. To do this it must first be granted an "Authorization Certificate" (often called an Registration Authority Certificate or Enrollment Agent certificate) to authenticate to the Certificate Authority.

CFAS cannot issue logon certificates if the CA administrator denies its request for an Authorization Certificate, or if its in the possession of expired / invalid certificates. Administrators should therefore track the status of every Authorization Certificate on CFAS and promptly isolate the ones that have expired, have been denied, or are invalid. The Citrix FAS Authorization Certificates test helps administrators with this!

The test auto-discovers all the Authorization Certificates on CFAS, and reports the current status of each certificate.

Target of the test : Citrix Federated Authentication Server

Agent deploying the test : An internal agent

Outputs of the test : One set of the results for each Authorization Certificate

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed. By default, this is set to 5 minutes.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens.
Detailed Diagnosis	<p>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.</p> <p>The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:</p> <ul style="list-style-type: none"> • 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		
Certificate status	Indicates the current status of this Authorization Certificate		The values that this measure reports and their corresponding numeric values are listed in the table below:		
			Measure Values	Numeric Values	Description

Measurement	Description	Measurement Unit	Interpretation												
			<table><tr><td>Ok</td><td>1</td><td></td></tr><tr><td>Maintenance Required</td><td>2</td><td></td></tr><tr><td>Maintenance Due</td><td>3</td><td></td></tr><tr><td>Expired</td><td>0</td><td></td></tr></table>	Ok	1		Maintenance Required	2		Maintenance Due	3		Expired	0	
Ok	1														
Maintenance Required	2														
Maintenance Due	3														
Expired	0														
			<p>Note:</p> <p>By default, this measure reports the Measure Values discussed above to indicate the status of an Authorization Certificate. In the graph of this measure however, the same is indicated using the numeric equivalents only.</p> <p>Using the detailed diagnosis of this measure, you can determine the details of the Authorization Certificate - this includes the certificate request, the CA to issue the certificate, and the storage container name (TrustArea).</p>												

3.1.2 Citrix FAS Authorization Definitions Test

To generate a user certificate, Citrix FAS requires different types of information such as:

- The CertificateTemplate to request;
- One/more loadbalanced/ failover Certificate Authority Addresses
- The ID of the AuthorizationCertificate to use to authorize the request
- A list of additional Issuance Policy OIDs to add to the certificate request
- A flag indicating if the certificate can be used as an in-session Virtual Smart Card, or only for the logon process

At any given point in time, an administrator can vett the configuration of a certificate by viewing the recipe for issuing that certificate - i.e., by viewing the Certificate Definition Objects. The Citrix

FAS Authorization Definitions test reports the definition of each certificate, thus enabling administrators to review the configuration and to figure out if anything is out of place.

Primarily, this test reveals which certificate can be used as an in-session Virtual Smart Card, and which can be used only for logging into the Citrix environment. The detailed diagnostics of the test on the other hand, sheds light on the other key certificate configurations such as the certificate template that is requested and the certificate authority addresses.

Target of the test : Citrix Federated Authentication Server

Agent deploying the test : An internal agent

Outputs of the test : One set of the results for each user certificate

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed. By default, this is set to 5 minutes.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens.
Detailed Diagnosis	<p>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.</p> <p>The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:</p> <ul style="list-style-type: none">• 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
Is in session?	Indicates whether/not this certificate can be used as		Certificates that have been configured

Measurement	Description	Measurement Unit	Interpretation						
	an in-session Virtual Smart Card.		<p>to be used as in-session certificates are placed in the user's personal certificate store after logon for application use. For example, if you require TLS authentication to web servers within the VDA session, the certificate can be used by Internet Explorer. By default, VDAs will not allow access to certificates after logon.</p> <p>If the certificate can be used as an in-session Virtual Smart Card, then this measure will report the value Yes. If the certificate can be used only at logon, then this measure will report the value No.</p> <p>The numeric values that correspond to these measure values are listed in the table below:</p> <table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table> <p>Note:</p> <p>By default, this measure will report the Measure Values listed in the table above to indicate whether/not the certificate can be used as an in-session Virtual Smart Card. However, in the graph of this measure, the same will be indicated using the numeric equivalents only.</p> <p>Use the detailed diagnosis of this measure to know the Microsoft certificate template that this certificate uses and the Certificate Authority Addresses.</p>	Measure Value	Numeric Value	Yes	1	No	0
Measure Value	Numeric Value								
Yes	1								
No	0								

3.1.3 Citrix FAS Details Test

The efficiency of Citrix FAS can be best evaluated by understanding its workload in terms of user sessions and certificate requests, and measuring how quickly it processes this workload. With the Citrix FAS Details test, administrators can do that and more!

This test reveals the count of active sessions on Citrix FAS and the count of concurrent certificate signing requests to it, thus providing administrators with a measure of the load on the server. The test further 'qualifies' the load as high, medium, and low, thereby enabling you to promptly detect overload conditions. Also, by reporting the average time taken by FAS to service the CSR requests and the rate at which requests are typically serviced, eG Enterprise reveals how efficiently FAS processes the requests. This way, eG Enterprise also brings processing bottlenecks to light.

Target of the test : Citrix Federated Authentication Server

Agent deploying the test : An internal agent

Outputs of the test : One set of the results for the Citrix FAS server being monitored

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed. By default, this is set to 5 minutes.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active sessions	Indicates the number of connections currently active on FAS.	Number	These are good measures of the current workload of the Citrix FAS server.
Concurrent CSRs	Indicates the number of certificate requests processed at the same time.	Number	
Private key operations performed	Reports the five minute rolling average of the	Number	

Measurement	Description	Measurement Unit	Interpretation								
	number of certificate private key operations being performed by the FAS.										
Request time	Indicates the length of time to generate and sign a certificate.	Seconds	Ideally, the value of this measure should be low. A consistent increase in the value of this measure is indicative of processing bottlenecks.								
Certificate count	Indicates the number of certificates being managed by the Federated Authentication Service.	Number									
Certificate signing request	Indicates the rate at which the certificate signing requests were processed.	Requests/min	Ideally, the value of this measure should be high. If this value dwindles with time, it is indicative of a processing bottleneck.								
High load	These are estimates of the load that FAS can accept in terms of 'CSRs per minute'.	Number									
Medium Load											
Low Load											
Estimated load	Indicates the estimated load factor.		<p>The values that this measure reports and the corresponding numeric values are listed in the table below:</p> <table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Low</td><td>0</td></tr><tr><td>Medium</td><td>1</td></tr><tr><td>High</td><td>2</td></tr></table> <p>Exceeding the “High Load” threshold may result in session launches failing.</p> <p>Note:</p> <p>By default, this measure will report the Measure Values listed in the table above to indicate the estimated load</p>	Measure Value	Numeric Value	Low	0	Medium	1	High	2
Measure Value	Numeric Value										
Low	0										
Medium	1										
High	2										

Measurement	Description	Measurement Unit	Interpretation
			factor. However, in the graph of this measure, the same will be indicated using the numeric equivalents only.

3.1.4 Citrix FAS MS Certificate Authority Details Test

A certification authority (CA) is responsible for attesting to the identity of users, computers, and organizations. The CA authenticates an entity and vouches for that identity by issuing a digitally signed certificate. The CA can also manage, revoke, and renew certificates.

Sometimes, one/more CAs in a domain may be unreachable for authenticating user logins. If user logins fail or if login authentication is delayed unduly, then administrators must be able to tell if it is owing to an inaccessible CA.

Also, when a certificate request is generated on CFAS using a template, the administration console sends it to a certificate authority that publishes that template. If a CA does not publish any template, very often it is because no requests were generated using any template that that CA publishes; not because, the CA could not be contacted. Administrators however, tend to wrongly attribute the absence of templates to publish to the unavailability of the CA. With the help of the Citrix FAS MS Certificate Authority Details test, administrators can finally set the record straight!

This test takes stock of all the CAs installed in the CFAS domain. The test then periodically checks whether/not every CA is accessible, and alerts administrators to the inaccessibility of any CA. This way, if a CA is not publishing templates, then administrators can figure out if it is because there are no templates to publish or because the CA is unreachable. Additionally, for each CA, the test reports whether/not it is the default/primary CA.

Target of the test : Citrix Federated Authentication Server

Agent deploying the test : An internal agent

Outputs of the test : One set of the results for each Microsoft CA installed in the CFAS domain

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed. By default, this is set to 5 minutes.
Host	The IP address of the host for which this test is to be configured.

Parameter	Description
Port	The port at which the specified host listens.
Domain, Username, Password	This test requires domain administrator privileges to run. Therefore, specify the name of domain to which the CFAS belongs against DOMAIN . Enter the credentials of the domain administrator against the USERNAME and PASSWORD text boxes.
Confirm Password	Confirm the password by retyping it here.
Detailed Diagnosis	<p>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.</p> <p>The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:</p> <ul style="list-style-type: none"> • 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						
Is microsoft certificate accessible?	Indicates whether/not the CA is accessible.		<p>If the CA is accessible, then this measure will report the value Yes. If the CA is inaccessible, then this measure will report the value No.</p> <p>The numeric values that correspond to the aforesaid measure values are as follows:</p> <table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table> <p>Note:</p> <p>By default, this measure will report the</p>	Measure Value	Numeric Value	Yes	1	No	0
Measure Value	Numeric Value								
Yes	1								
No	0								

Measurement	Description	Measurement Unit	Interpretation
			<p>Measure Values listed in the table above to indicate whether/not the certificate can be used as an in-session Virtual Smart Card. However, in the graph of this measure, the same will be indicated using the numeric equivalents only.</p> <p>Use the detailed diagnosis of this measure to know which templates were published by the CA.</p>
Is it default microsoft certificate?	Indicates whether/not this CA is the default/primary CA.		

3.1.5 Citrix FAS Servers Test

After you install the Citrix Federated Authentication Service on a server, you must specify the full DNS addresses of the FAS servers in Group Policy. At any later point in time, an administrator can modify the details of FAS servers configured via Group Policy, using the Set-FasServer powershell cmdlet. In particular, the administrator can enable/disable maintenance mode for a FAS server, so that the server rejects new connections (callers will fail over to different FAS servers).

To know which FAS servers configured via Group Policy have maintenance mode enabled, use the Citrix FAS Servers test.

This test discovers the FAS servers that have been configured via Group Policy and reports whether/not the maintenance mode has been enabled on every FAS server.

Target of the test : Citrix Federated Authentication Server

Agent deploying the test : An internal agent

Outputs of the test : One set of the results for each FAS server configured via Group Policy

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed. By default, this is set to 5 minutes.

Parameter	Description
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens.
Detailed Diagnosis	<p>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.</p> <p>The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:</p> <ul style="list-style-type: none"> • 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						
Is in maintenance mode?	Indicates whether/not maintenance mode is enabled on this FAS server.		<p>If maintenance mode is enabled on a FAS server, then this measure will report the value Yes. If the maintenance mode is disabled, then this measure will report the value No.</p> <p>The numeric values that correspond to the aforesaid measure values are as follows:</p> <table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table> <p>Note:</p> <p>By default, this measure will report the Measure Values listed in the table above to indicate whether/not maintenance mode is enabled.</p>	Measure Value	Numeric Value	Yes	1	No	0
Measure Value	Numeric Value								
Yes	1								
No	0								

Measurement	Description	Measurement Unit	Interpretation
			<p>However, in the graph of this measure, the same will be indicated using the numeric equivalents only.</p> <p>Use the detailed diagnosis of this measure to know the FAS version and the index number that the Group Policy object has added to the FAS server.</p>

3.1.6 Citrix FAS User Certificate Details Test

Citrix FAS authorizes users to login to the Citrix environment by issuing certificates to the users. To know how many users were issued certificates and what fraction of these certificates are expired, use the Citrix FAS User Certificate Details test.

This test monitors the user certificates managed by Citrix FAS, tracks the usage of these certificates, and reports the count of users who were issued certificates. The test also reports the number of expired certificates, with detailed diagnosis throwing light on which certificates expired and when.

Target of the test : Citrix Federated Authentication Server

Agent deploying the test : An internal agent

Outputs of the test : One set of the results for the Citrix FAS server being monitored

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed. By default, this is set to 5 minutes.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens.
Show Total User DD	The detailed diagnosis of the <i>Total Users</i> measure, if enabled, provides detailed information regarding all certificates that Citrix FAS issued to users. In a typical Citrix environment, the Citrix FAS could be managing certificates for hundreds or even thousands of users. In such environments, the detailed metrics of the <i>Total Users</i> measure, if collected, may put considerable strain on the eG database. This is why, by default, eG Enterprise DOES NOT provide detailed metrics for the <i>Total Users</i> measure. Accordingly, the SHOW TOTAL USER DD flag is set to No . However, if you have a well-sized, well-tuned eG database, then you can set this flag to Yes , and

Parameter	Description
	enable the collection of detailed diagnostics for the <i>Total Users</i> measure.
Detailed Diagnosis	<p>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.</p> <p>The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:</p> <ul style="list-style-type: none"> • 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
Total users	Indicates the total number of users who were issued certificates.	Number	By default, the test does not collect detailed metrics for this measure. However, if the SHOW TOTAL USERS DD flag is set to Yes, then detailed diagnostics will be reported for this measure. Such detailed insights include the definition, expiry date, role, and thumbprint of every certificate managed by the Citrix FAS.
Total unique users	Indicates the unique users who were issued certificates.	Number	
Total expired users	Indicates the total number of users whose certificates have expired.	Number	Use the detailed diagnosis of this measure to determine which certificates expired and when.
Total unique expired users	Indicates the total number of unique users whose certificates have expired.	Number	

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.

Copyright © 2018 eG Innovations Inc. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations 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. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.