GEMINI USER GUIDE

Changes Introduced as part of XRN5368.2

Covered in this Document

Single Sign-On (SSO)

Access Over the Internet

Multi-Factor Authentication (MFA)

Self-Service Password Reset (SSPR)

Table of Contents

Introduction

A change proposal (XRN5368) was received from National Grid to progress a number of sustain and optimisation activities associated with the Gemini system. A few elements of this were taken under XRN5368.2 – Single Sign-On (SSO) Project. The purpose of this User Guide is to go through how these updates have affected the user experience when accessing Gemini.

As an overview, this project covers the below:

Single Sign-On (SSO): This change has simplified the log-in process for Gemini online screens, removing the need for users to manage two sets of credentials (Gemini Citrix & Gemini Application). Following the change, logging in with a Gemini Citrix username & password will automatically log the user into the Gemini Application layer.

Access Over the Internet: In addition to the current access via the IX link, Gemini has now been published over the internet via a different URL. This will act as a replacement for the current XP1 back-up access. End of support for the XP1 tokens is due at the end of June 2022.

Multi-Factor Authentication (MFA): As an additional layer of security for those accessing via the newly created internet link, users will be asked to authenticate using an application-based MFA method. This additional step with prompt you for an additional One-Time-Passcode (OTP) which will be displayed on your chosen device.

Self-Service Password Reset (SSPR): It is now possible to reset Gemini passwords from the Gemini Self-Service Portal. Local Security Officers (LSOs) will no longer be required to contact the Service Desk for password resets, but this option is still available if required.

If you are facing any issues with any of the new functionality then please don’t hesitate to contact our Service Desk on **0845 600 0506** or via email to **servicedesk@xoserve.com**. Alternatively you can raise a ticket via our portal using this **link**.

Single Sign-On (SSO)

Prior to this change, Gemini users followed a complex log-in process that involved logging-in with both Citrix and the Gemini application IDs - this required maintaining and remembering two sets of credentials. The introduction of a Single Sign-On functionality removes the need for users having to manage two credentials and has simplified the Gemini log-in process.

Pre-requisites

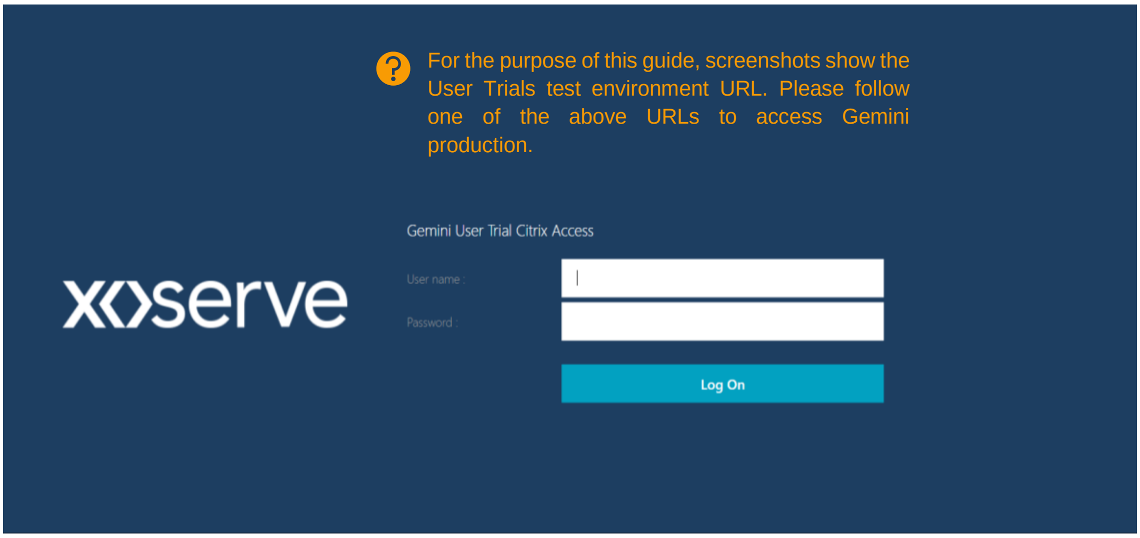
Gemini users will not need to register or apply any changes to use this functionality, however they will need to ensure the following criteria are met:

- Users will need matching Gemini Citrix and Gemini Application IDs.
- Gemini Citrix and Gemini Application IDs should both be active (not expired).

Using Single Sign-On (Step by Step)

1) Launch the Gemini URL using your preferred browser. You can either use the existing URL which will take you via the IX link or try our newly published internet-facing URL (MFA will be required in this case).

IX Route:	https://prod-ix-citrix.geminints.com
Internet Route:	https://prod-int-citrix.geminiwebservices.com



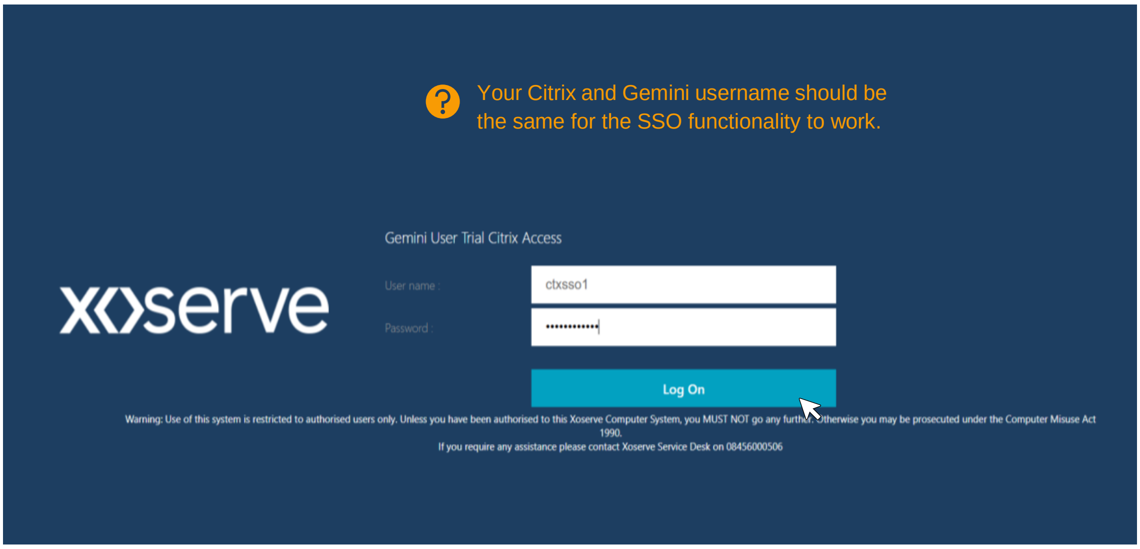
For the purpose of this guide, screenshots show the User Trials test environment URL. Please follow one of the above URLs to access Gemini production.

Gemini User Trial Citrix Access

User name : |

Password :

2) Enter your Gemini Citrix username and password and click the Log On button. If your password has expired, you will first need to reset the password via your preferred route.



Your Citrix and Gemini username should be the same for the SSO functionality to work.

Gemini User Trial Citrix Access

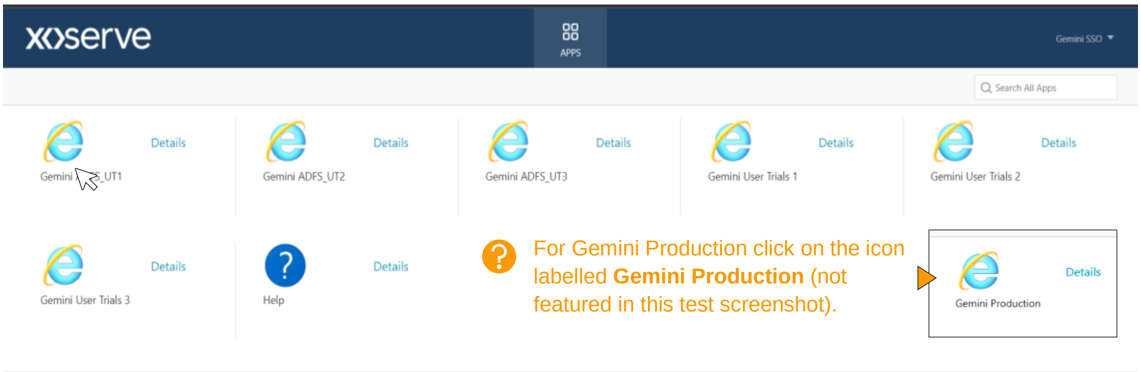
User name : ctxsso1

Password : ••••••••••••

Warning: Use of this system is restricted to authorised users only. Unless you have been authorised to this Xoserve Computer System, you MUST NOT go any further. Otherwise you may be prosecuted under the Computer Misuse Act 1990.

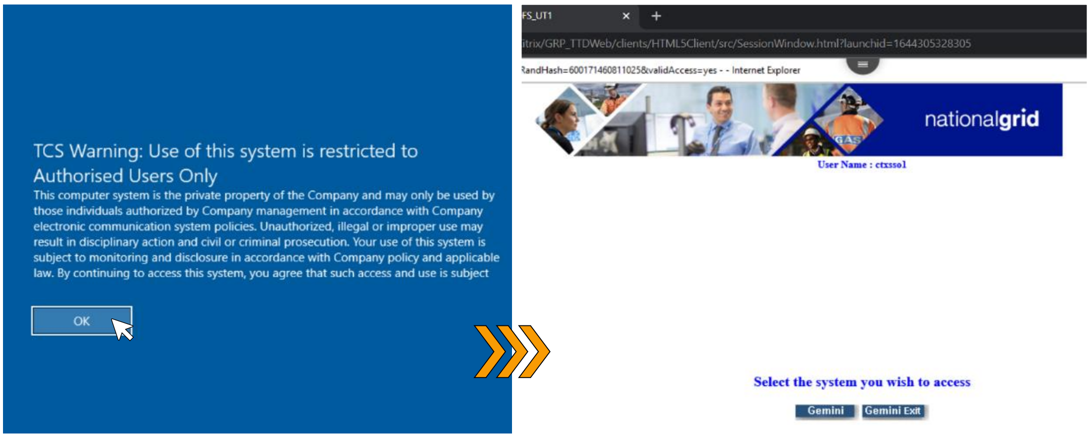
If you require any assistance please contact Xoserve Service Desk on 08456000506

3) Upon successful entry to the Gemini Citrix homepage, click the Gemini environment you wish to access. For Gemini Production, this icon will be labelled **Gemini Production**.



For Gemini Production click on the icon labelled **Gemini Production** (not featured in this test screenshot).

4) Click the OK button and the Single Sign-On functionality will enter you directly into Gemini application without prompting for additional credentials.



TCS Warning: Use of this system is restricted to Authorised Users Only

This computer system is the private property of the Company and may only be used by those individuals authorized by Company management in accordance with Company electronic communication system policies. Unauthorized, illegal or improper use may result in disciplinary action and civil or criminal prosecution. Your use of this system is subject to monitoring and disclosure in accordance with Company policy and applicable law. By continuing to access this system, you agree that such access and use is subject

FS_UT1

itrix/GRP_TTDWeb/clients/HTML5Client/src/SessionWindow.html?launchid=1644305328305

RandHash=600171460811025&validAccess=yes - - Internet Explorer

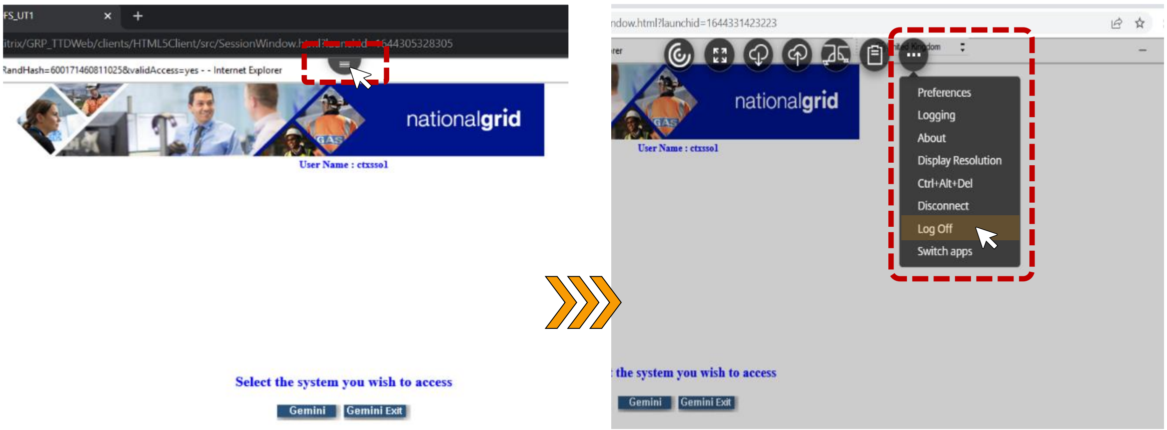
User Name : ctxsso1

Select the system you wish to access

Note: For this functionality to work, users must have matching Gemini Citrix and Gemini Application IDs - both must also be active.

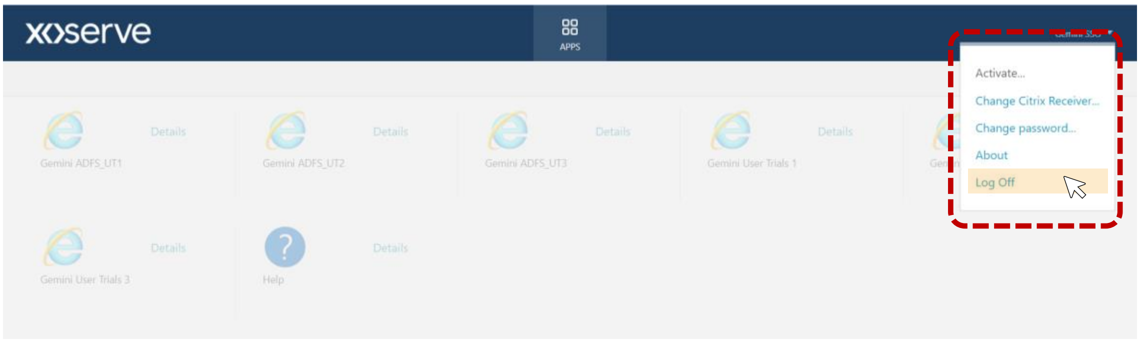
5) To log-off, first click on the Citrix workspace menu at the top of your screen. Once in the menu, click on the three dots and select Log Off from the drop-down menu.

Note: It is important to log-off properly from the system to ensure the session is correctly closed. Failure to do this can cause the session to be stuck and result in you not being able to launch the application in the future – this scenario must be resolved via our Service Desk.



Select the system you wish to access

6) Click the Gemini SSO drop down in the Citrix homepage and select the Log Off option from the list.



Access Over the Internet & Multi-Factor Authentication

The primary method for accessing Gemini for most users will be via the IX link. Whilst this route is still be available, it is now also possible to log-in to Gemini over the internet with the newly published internet-facing URL.

This removes the requirement for XP1 tokens (used as a back-up solution) ahead of their end of support date at the end of June 2022. After the XP1 tokens have been decommissioned, this route will act as the permanent replacement for those wishing to access Gemini via the contingency route.

Accessing over the internet route brings an additional layer of security in the form of Multi-Factor Authentication (MFA). This additional step helps us verify the identity of the user with a One-Time-Passcode (OTP). This is delivered via either the Google Authenticator or Microsoft Authenticator mobile applications.

Pre-requisites

Gemini users wishing to access the system via this new route will need to make sure the below requirements are met:

- Set up the Multi-Factor Authentication using your preferred device. Details on how to do this can be found in the next section.
- When accessing over this URL, ensure you have your MFA device with you, so you can enter the One-Time-Passcode (OTP).
- Ensure the new URL is not blocked by your company firewall, proxy agent or VPN solution.

Setting Up Your Multi-Factor Authentication (Step by Step)

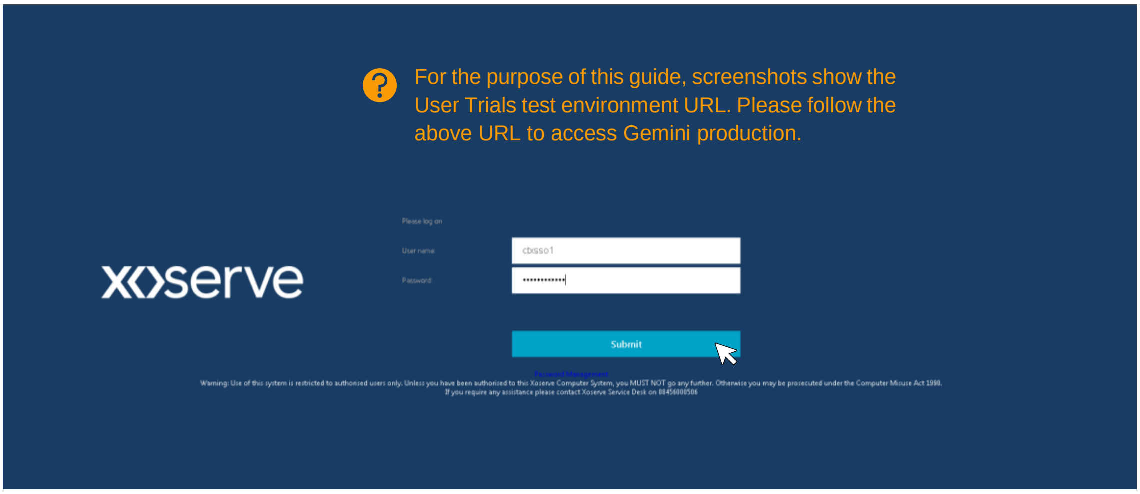
1) Download either the Google Authenticator or Microsoft Authenticator application on your preferred device. It is possible to add/remove devices after setup but be aware you will need your device (phone, tablet etc) with you when you log into Gemini via this route.

Note: In this guide we will predominantly show the Microsoft Authenticator app as a reference. If you are using the Google Authenticator app, this may look different, but the functionality will remain the same.

2) Launch the MFA registration URL using your preferred desktop browser, with the link below.

MFA Registration: https://prod-int-citrix.geminiwebservices.com/manageotp

3) Enter your Gemini Citrix username and password and click the Submit button.



For the purpose of this guide, screenshots show the User Trials test environment URL. Please follow the above URL to access Gemini production.

xoserve

Please log on

User name: cbsso1

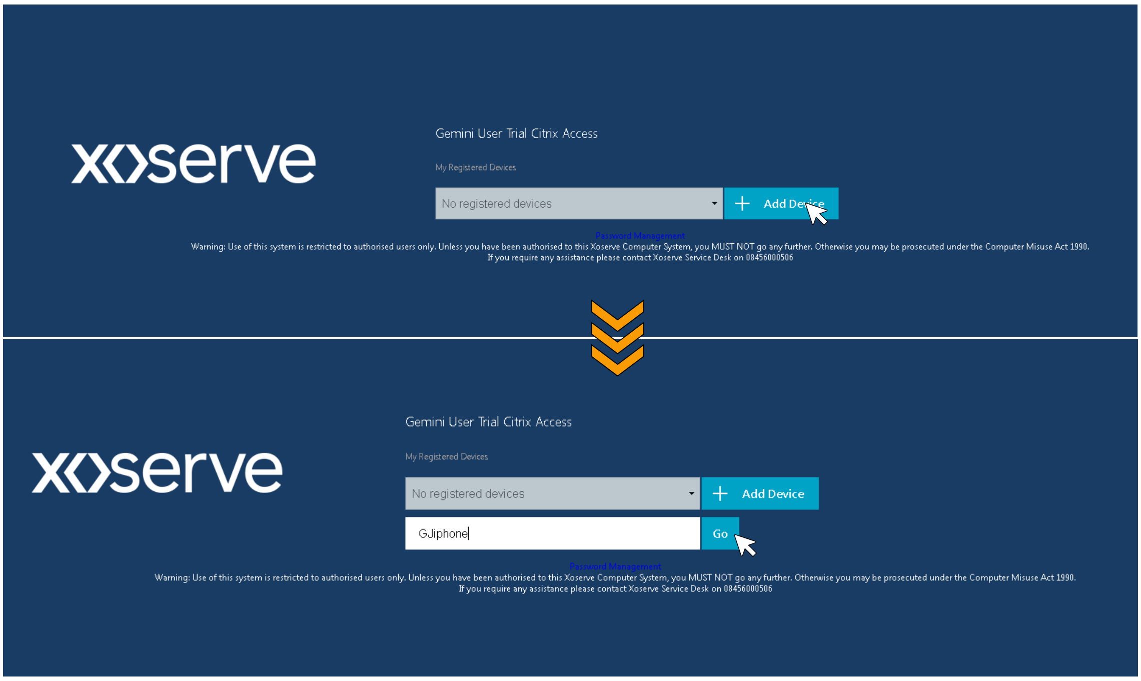
Password: ••••••••••••

Submit

Password Management

Warning: Use of this system is restricted to authorised users only. Unless you have been authorised to this Xoserve Computer System, you MUST NOT go any further. Otherwise you may be prosecuted under the Computer Misuse Act 1990.
If you require any assistance please contact Xoserve Service Desk on 08456000506

4) Once your credentials have been successfully validated, you will see the device registration page. Click the Add Device button and name the device something appropriate – this name will help you keep track of your registered devices.



xoserve

Gemini User Trial Citrix Access

My Registered Devices

No registered devices

+ Add Device

Password Management

Warning: Use of this system is restricted to authorised users only. Unless you have been authorised to this Xoserve Computer System, you MUST NOT go any further. Otherwise you may be prosecuted under the Computer Misuse Act 1990.
If you require any assistance please contact Xoserve Service Desk on 08456000506

xoserve

Gemini User Trial Citrix Access

My Registered Devices

No registered devices

+ Add Device

GJiphone

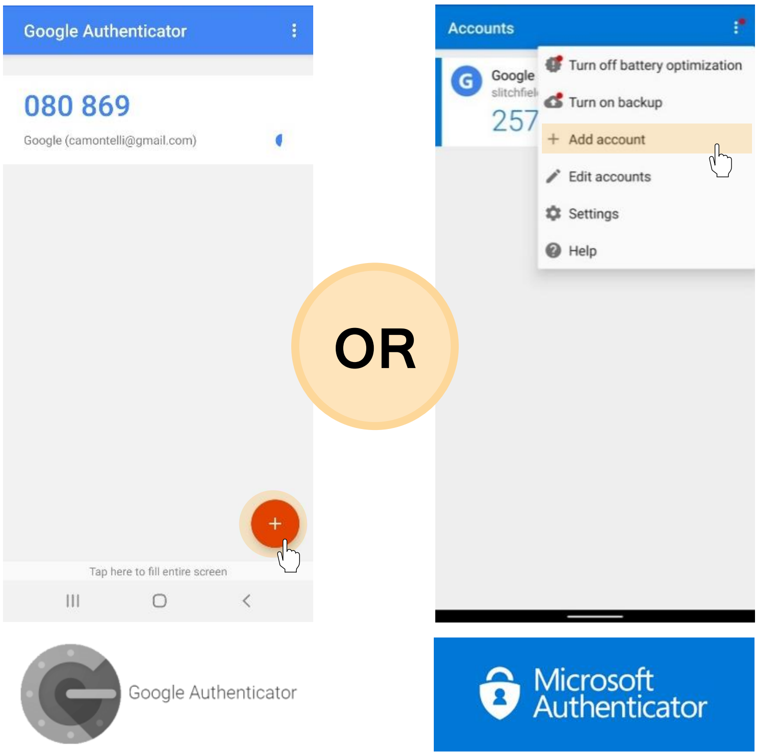
Go

Password Management

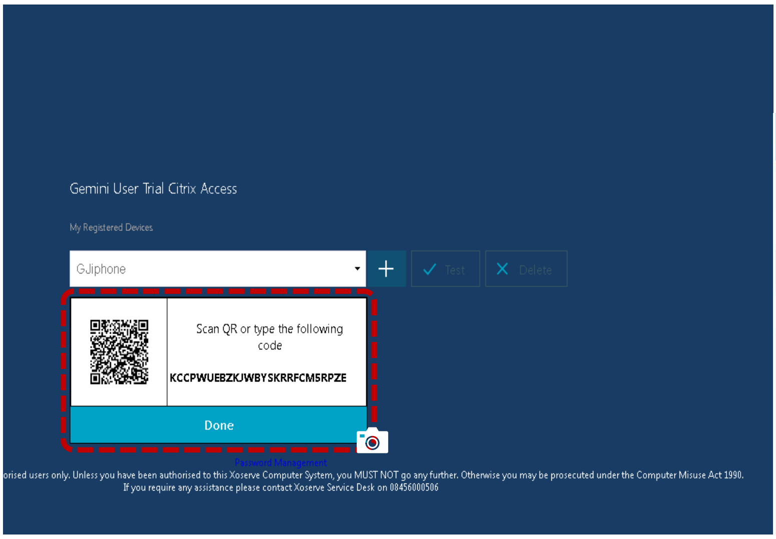
Warning: Use of this system is restricted to authorised users only. Unless you have been authorised to this Xoserve Computer System, you MUST NOT go any further. Otherwise you may be prosecuted under the Computer Misuse Act 1990.
If you require any assistance please contact Xoserve Service Desk on 08456000506

5) Open the authenticator app on your mobile device (Google or Microsoft) and then tap the add account button. For the Microsoft Authenticator app you will have to navigate via the three dots in the top right of the screen. To add an account via the Google Authenticator app, simply tap the big plus in the bottom right.

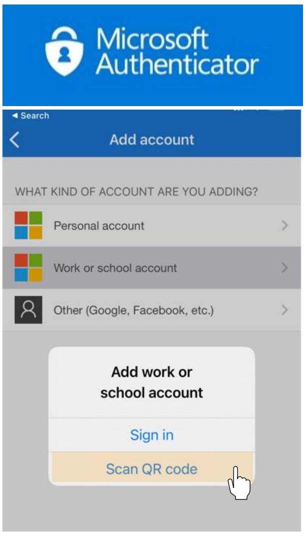
Note: The exact layout for these apps will change based on the device and when the software is updated over time.



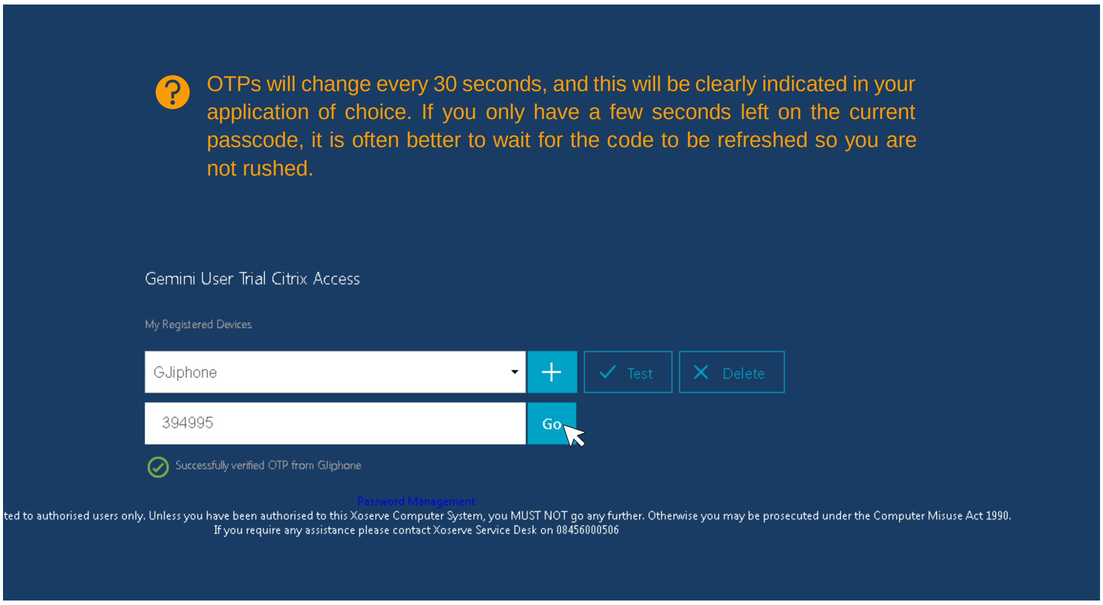
6) If you are using the Microsoft Authenticator app you can select the type of account you want to add. For both apps, you then select the Scan a QR Code option and scan the QR code using the camera on your device.


Gemini User Trial Citrix Access
My Registered Devices
GJiphone
Test
Delete
Scan QR or type the following code
KCCPWUEBZKJWBYSKRRFCM5RPZE
Done
Password Management

orised users only. Unless you have been authorised to this Xoserve Computer System, you MUST NOT go any further. Otherwise you may be prosecuted under the Computer Misuse Act 1990.
If you require any assistance please contact Xoserve Service Desk on 08456000506



7) Once registered, click on the Test button in your browser and enter the One-Time-Passcode (OTP) that has appeared on your device. Click the Go button and you will see that the device has been successfully tested.



OTPs will change every 30 seconds, and this will be clearly indicated in your application of choice. If you only have a few seconds left on the current passcode, it is often better to wait for the code to be refreshed so you are not rushed.

Gemini User Trial Citrix Access

My Registered Devices

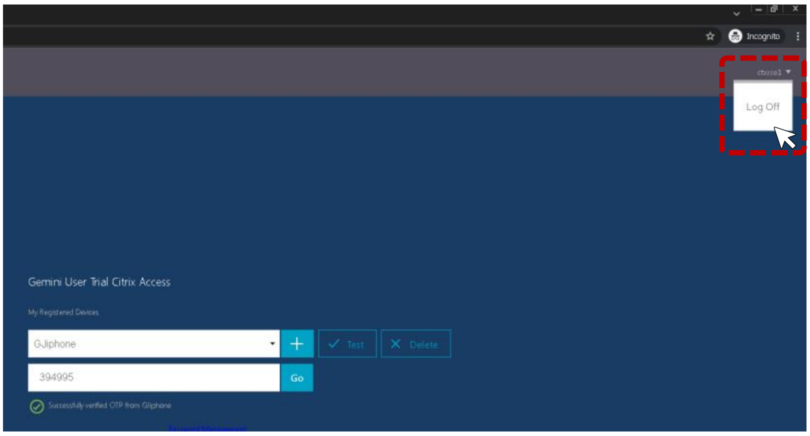
GJiphone

394995

Successfully verified OTP from GJiphone

ted to authorised users only. Unless you have been authorised to this Xoserve Computer System, you MUST NOT go any further. Otherwise you may be prosecuted under the Computer Misuse Act 1990.
If you require any assistance please contact Xoserve Service Desk on 08456000506

8) To return to the log in page and use your newly registered MFA device, simply log off via the Citrix menu. Click the Log On button to return to the Citrix log-in page.



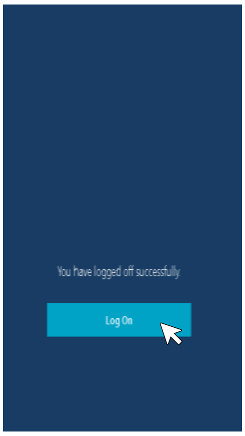
Gemini User Trial Citrix Access

My Registered Devices

GJiphone

394995

Successfully verified OTP from GJiphone



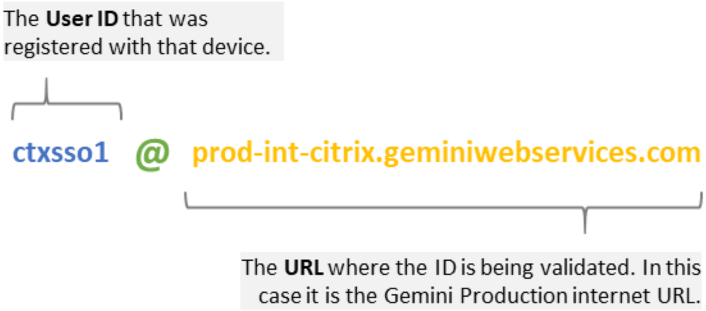
You have logged off successfully

Access Over the Internet (Step by Step)

1) Launch the Gemini Internet URL using your preferred browser. Whilst the existing IX link route is still available, this part of the guide is focused on access via the new internet-facing URL. To access via this route, you will need to use your registered MFA mobile device – if you have not yet registered a device please go to the previous section and follow the steps.

Internet Route: https://prod-int-citrix.geminiwebservices.com

2) Open the authenticator application (Microsoft or Google) on your chosen mobile device. If you have multiple MFA functionality on that device, you may have to select the account that is linked to Gemini. If you are having trouble identifying the correct code, it will usually be labelled using the syntax below.

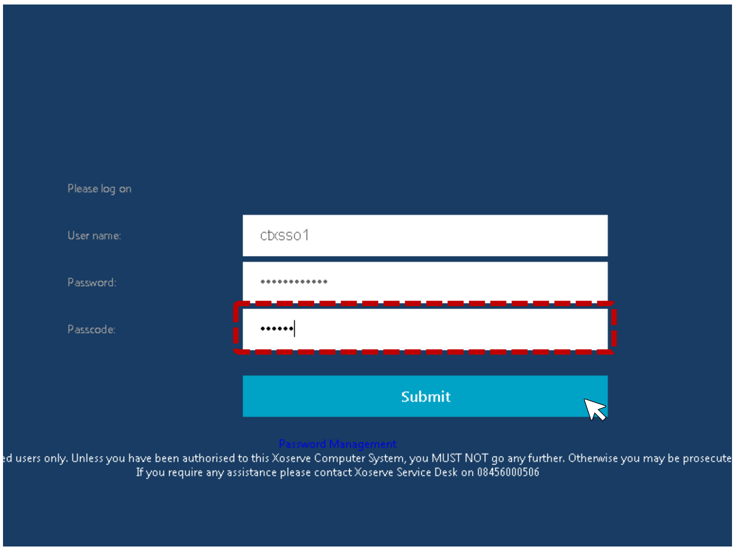


The **User ID** that was registered with that device.

ctxsso1 @ prod-int-citrix.geminiwebservices.com

The **URL** where the ID is being validated. In this case it is the Gemini Production internet URL.

3) In your desktop browser, you will be faced with a similar Citrix log-in page but with an additional box labelled Passcode. Enter your Citrix username and password as normal, then enter the One-Time-Passcode (OTP) displayed on your authenticator app. Click the Submit button to enter the Citrix homepage.



Please log on

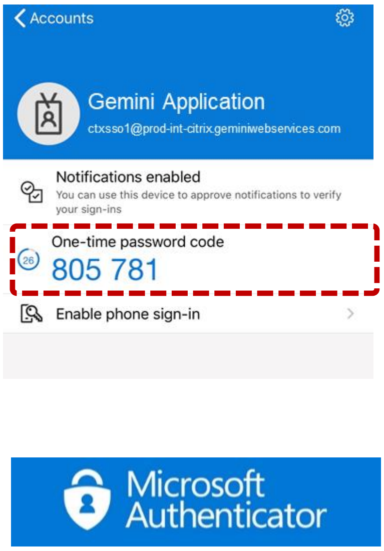
User name: ctxsso1

Password: ••••••••••••

Passcode: ••••••

ed users only. Unless you have been authorised to this Xoserve Computer System, you MUST NOT go any further. Otherwise you may be prosecute

If you require any assistance please contact Xoserve Service Desk on 08456000506



Gemini Application

ctxsso1@prod-int-citrix.geminiwebservices.com

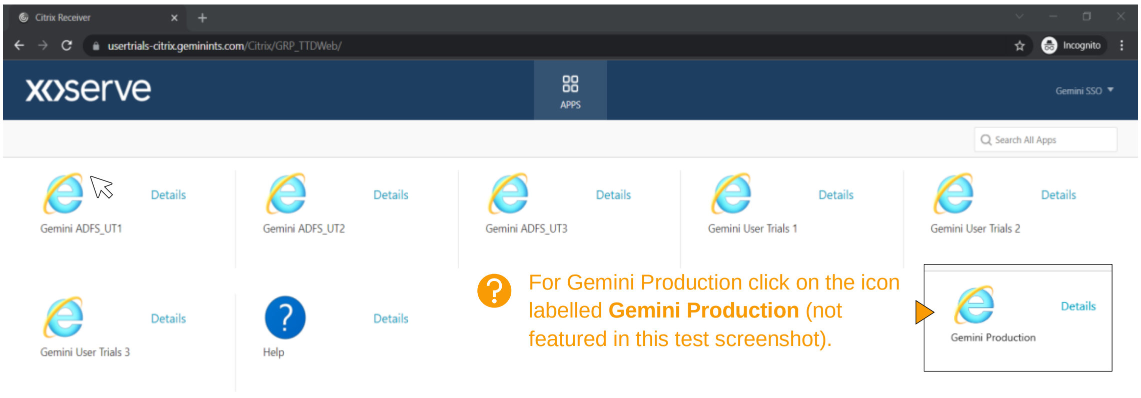
Notifications enabled

You can use this device to approve notifications to verify your sign-ins

One-time password code

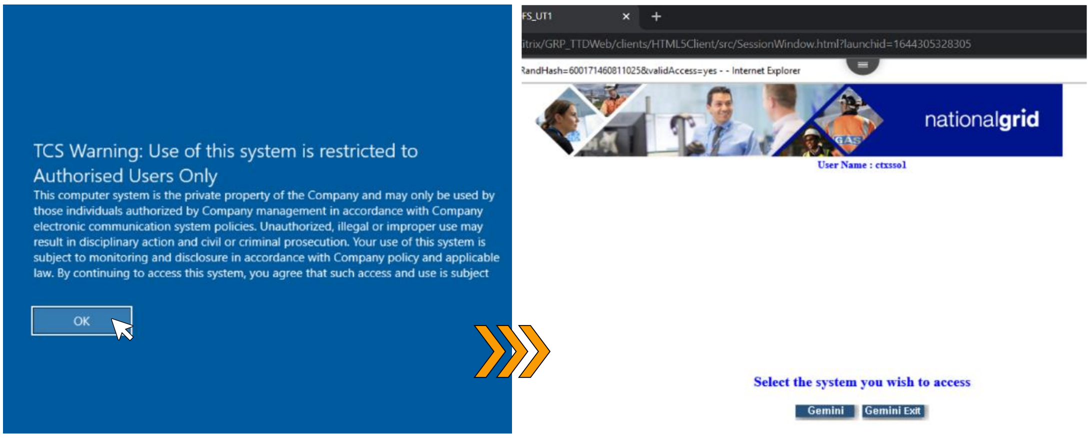
805 781

4) Upon successful entry to the Gemini Citrix homepage, click the Gemini environment you wish to access. For Gemini Production, this icon will be labelled Gemini Production.



For Gemini Production click on the icon labelled **Gemini Production** (not featured in this test screenshot).

5) Click the OK button and the Single Sign-On functionality will enter you directly into Gemini application without prompting for additional credentials.



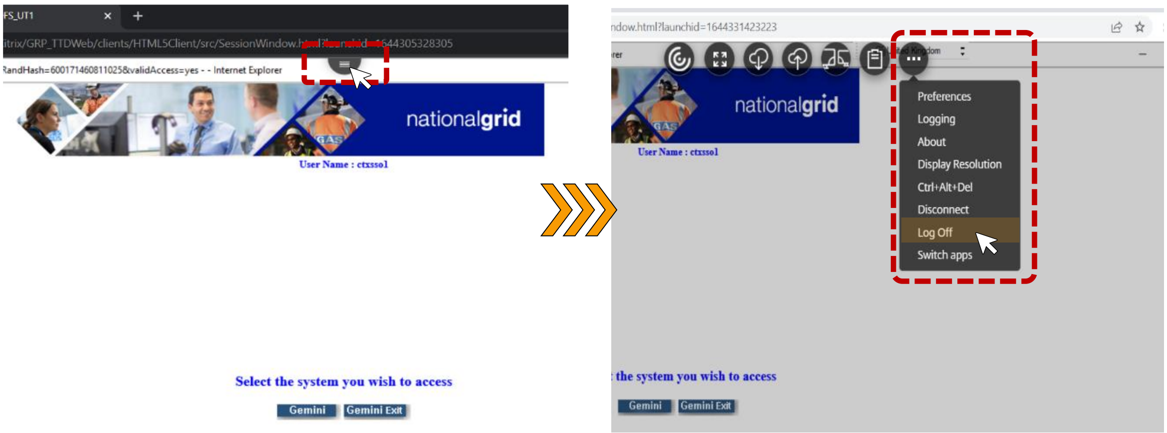
TCS Warning: Use of this system is restricted to Authorised Users Only

This computer system is the private property of the Company and may only be used by those individuals authorized by Company management in accordance with Company electronic communication system policies. Unauthorized, illegal or improper use may result in disciplinary action and civil or criminal prosecution. Your use of this system is subject to monitoring and disclosure in accordance with Company policy and applicable law. By continuing to access this system, you agree that such access and use is subject

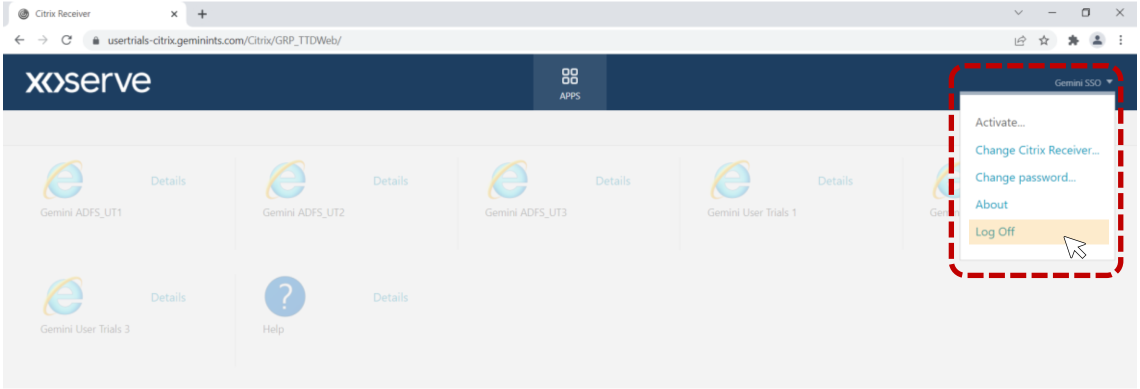
OK
FS_UT1
itrix/GRP_TTDWeb/clients/HTML5Client/src/SessionWindow.html?launchid=1644305328305
RandHash=6001714608110258validAccess=yes - - Internet Explorer
nationalgrid
User Name : ctxssol
Select the system you wish to access
Gemini
Gemini Exit

6) To log-off, first click on the Citrix workspace menu at the top of your screen. Once in the menu, click on the three dots and select Log Off from the drop-down menu.

Note: It is important to log-off properly from the system to ensure the session is correctly closed. Failure to do this can cause the session to be stuck and result in you not being able to launch the application in the future – this scenario must be resolved via our Service Desk.


FS_UT1
itrix/GRP_TTDWeb/clients/HTML5Client/src/SessionWindow.html?launchid=1644305328305
RandHash=6001714608110258validAccess=yes - - Internet Explorer
nationalgrid
User Name : ctxssol
Select the system you wish to access
Gemini
Gemini Exit
ndow.html?launchid=1644331423223
Preferences
Logging
About
Display Resolution
Ctrl+Alt+Del
Disconnect
Log Off
Switch apps
the system you wish to access

7) Click the Gemini SSO drop down in the Citrix homepage and select the Log Off option from the list.



Self-Service Password Reset (SSPR)

Previously, Gemini Citrix or Application password resets had to be raised with our Service Desk by an organisation’s dedicated Local Security Officer (LSO). Now, regardless of which route the user chooses to access Gemini, they have access to the Self-Service Password Reset functionality to reduce the effort required to manage Gemini accounts.

The SSPR function is delivered at the Citrix layer, and password updates are pushed through to the Gemini application layer. This means that the Gemini application password is kept in-sync with Gemini Citrix password, removing the need to reset the credentials separately. If required, existing password reset options are still available.

To access this tool, users will have to log-in to a separate Self-Service Portal, with an additional layer of security in the form of Multi-Factor Authentication.

Pre-requisites

Gemini users who want to make use of the SSPR functionality will need to make sure the below requirement is met:

- Register for the Self-Service Password Reset using your preferred device. Details on how to do this can be found in the next section.
- Ensure the new URL is not blocked by your company firewall, proxy agent or VPN solution.

Setting Up Your Self-Service Portal using an Authenticator Application (Step by Step)

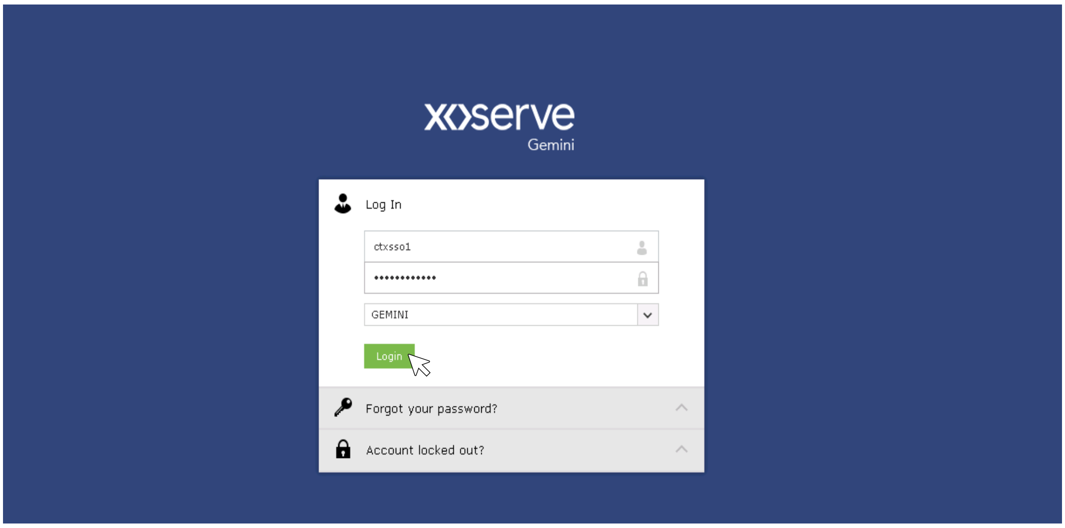
1) Download either the Google Authenticator or Microsoft Authenticator application on your preferred device. It is possible to add/remove devices after setup but be aware you will need your device (phone, tablet etc) with you when you access the portal.

Note: In this guide we will predominantly show the Microsoft Authenticator app as a reference. If you are using the Google Authenticator app, this may look different, but the functionality will remain the same.

2) Launch the SSPR registration URL using your preferred desktop browser, with the link below. Alternatively, you can access via the Password Management hyperlink on the Gemini Citrix log-in page.

SSPR Registration: https://selfservice.geminiwebservices.com/

3) Enter your Gemini Citrix username and password and click the Log In button.

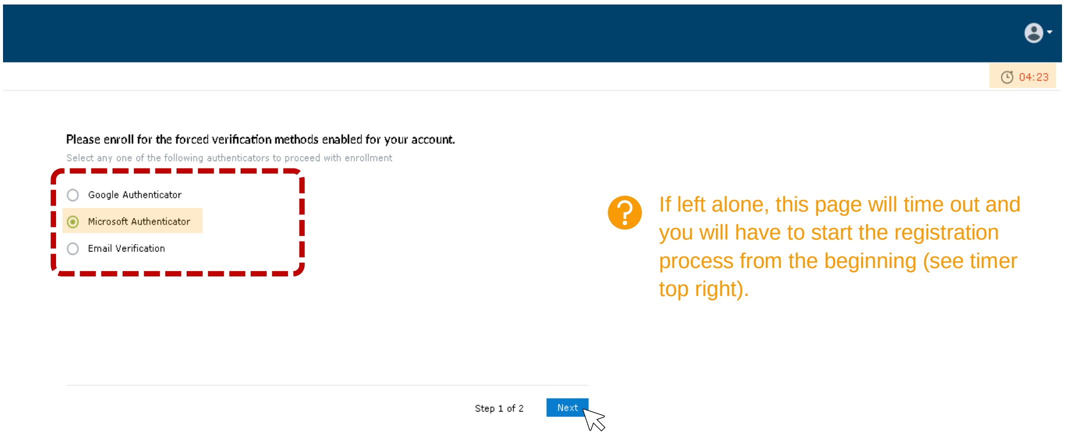


ctxsso1

••••••••••••

GEMINI

4) Select your preferred authentication method from the options and ensure this matches the application that is installed on your device.



Please enroll for the forced verification methods enabled for your account.

Select any one of the following authenticators to proceed with enrollment

○ Google Authenticator

● Microsoft Authenticator

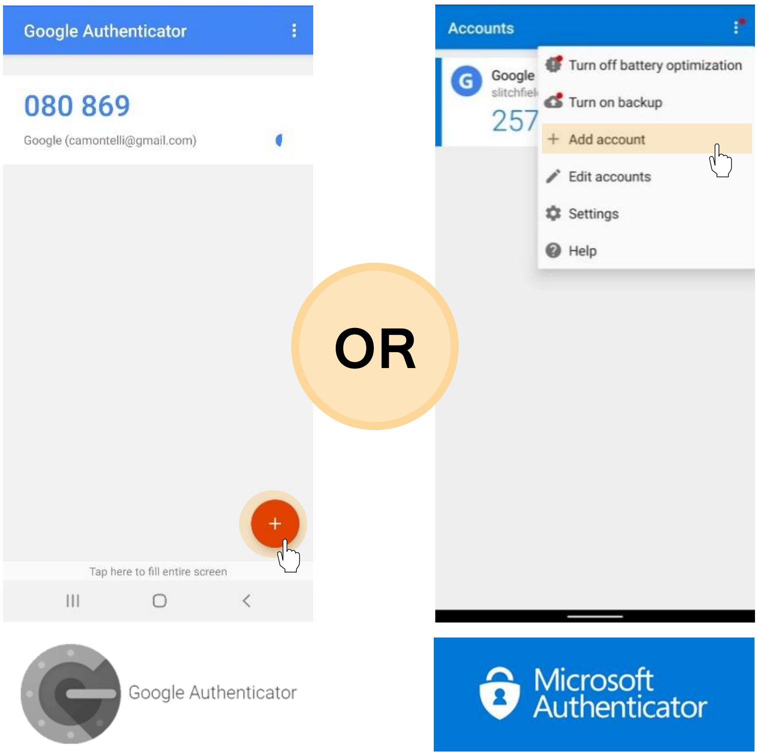
○ Email Verification

Step 1 of 2

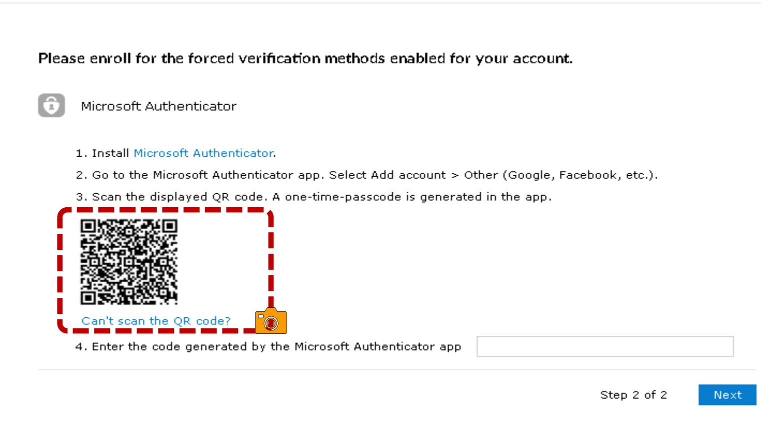
If left alone, this page will time out and you will have to start the registration process from the beginning (see timer top right).

5) Open the authenticator app on your mobile device (Google or Microsoft) and tap the add account button. For the Microsoft Authenticator app you will have to navigate via the three dots in the top right of the screen. To add an account via the Google Authenticator app, simply tap the big plus in the bottom right.

Note: The exact layout for these apps will change based on the device and when the software is updated over time.



6) If you are using the Microsoft Authenticator app you can select the type of account, you want to add. For both apps, you then select the Scan a QR Code option and scan the QR code using the camera on your device.



Please enroll for the forced verification methods enabled for your account.

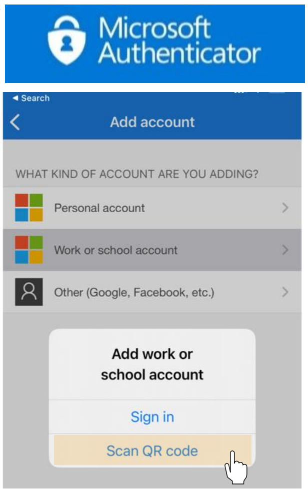
Microsoft Authenticator

1. Install Microsoft Authenticator.
2. Go to the Microsoft Authenticator app. Select Add account > Other (Google, Facebook, etc.).
3. Scan the displayed QR code. A one-time-passcode is generated in the app.

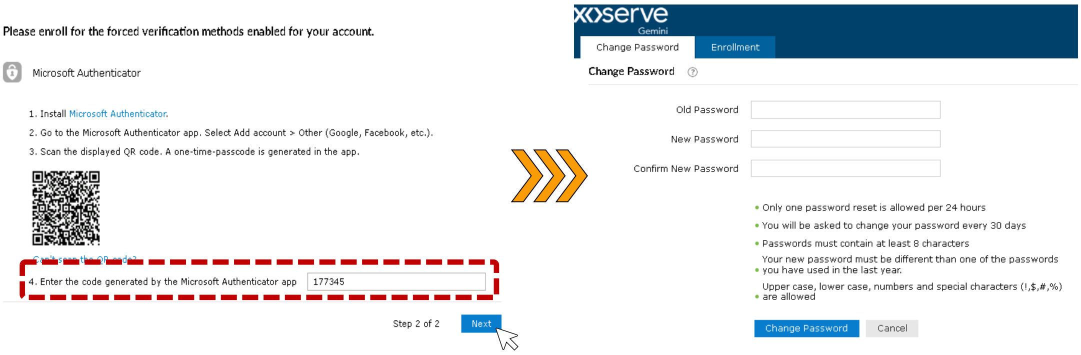
Can't scan the QR code?

4. Enter the code generated by the Microsoft Authenticator app

Step 2 of 2 Next



7) Enter the One-Time-Passcode (OTP) that appears in the authenticator application, on your mobile device. Click Next to complete the device registration and the Change Password tab will now be available.



Please enroll for the forced verification methods enabled for your account.

Microsoft Authenticator

1. Install Microsoft Authenticator.
2. Go to the Microsoft Authenticator app. Select Add account > Other (Google, Facebook, etc.).
3. Scan the displayed QR code. A one-time-passcode is generated in the app.

Can't scan the QR code?

4. Enter the code generated by the Microsoft Authenticator app: 177345

Step 2 of 2

Change Password

Old Password:

New Password:

Confirm New Password:

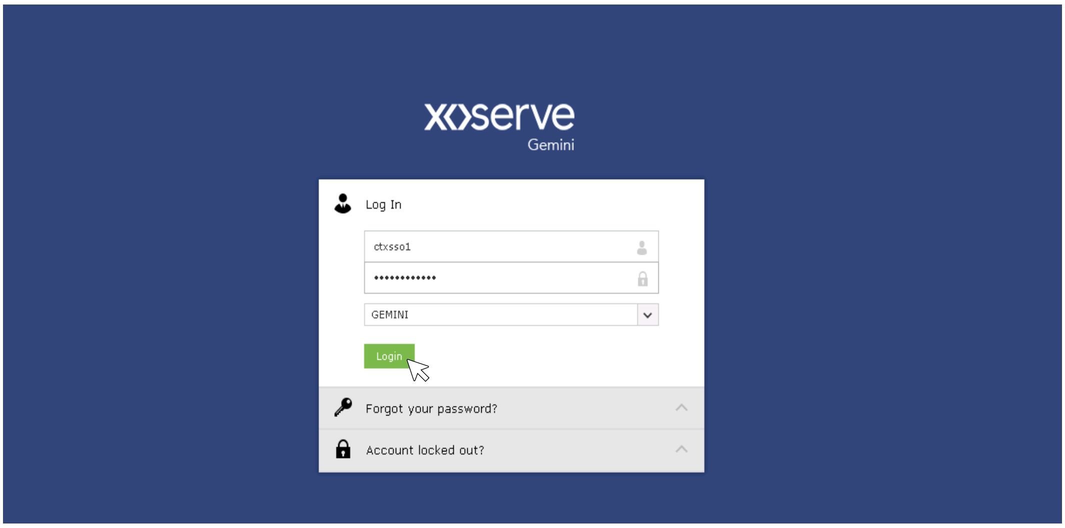
- Only one password reset is allowed per 24 hours
- You will be asked to change your password every 30 days
- Passwords must contain at least 8 characters
- Your new password must be different than one of the passwords you have used in the last year.
- Upper case, lower case, numbers and special characters (!,$,#,%) are allowed

Setting Up Your Self-Service Password Reset using an Email Account (Step by Step)

1) Launch the SSPR registration URL using your preferred desktop browser, with the link below.

SSPR Registration: https://selfservice.geminiwebservices.com/

2) Enter your Gemini Citrix username and password as normal and click the Log In button.



xoserve Gemini

Log In

ctxsso1

••••••••••••

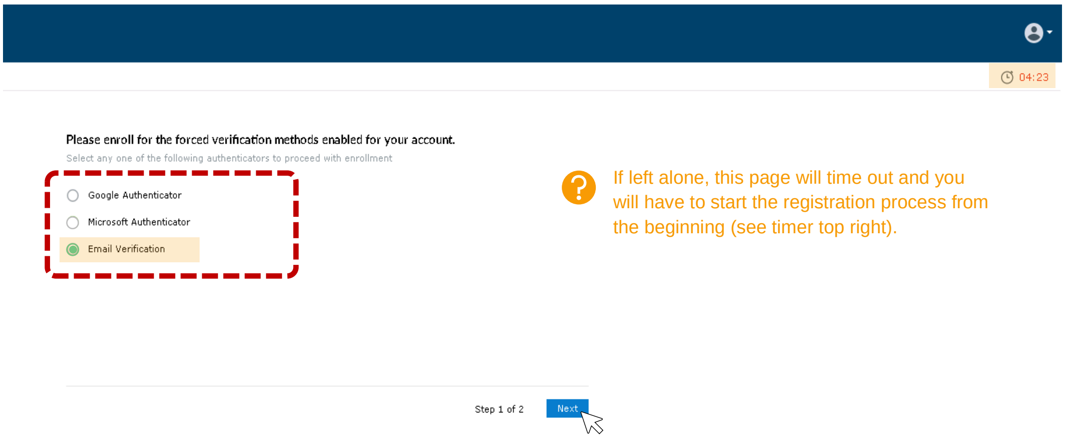
GEMINI

Login

Forgot your password?

Account locked out?

3) Select the Email Verification authentication method from the options and click on the Next button.



04:23

Please enroll for the forced verification methods enabled for your account.

Select any one of the following authenticators to proceed with enrollment

○ Google Authenticator

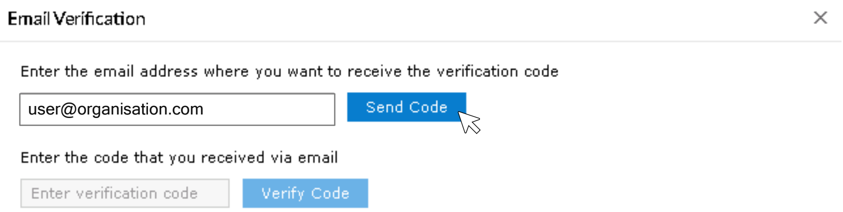
○ Microsoft Authenticator

● Email Verification

If left alone, this page will time out and you will have to start the registration process from the beginning (see timer top right).

Step 1 of 2 Next

4) Enter your work email ID and click the Send Code button to receive the One-Time-Passcode (OTP) to your email inbox.



Email Verification

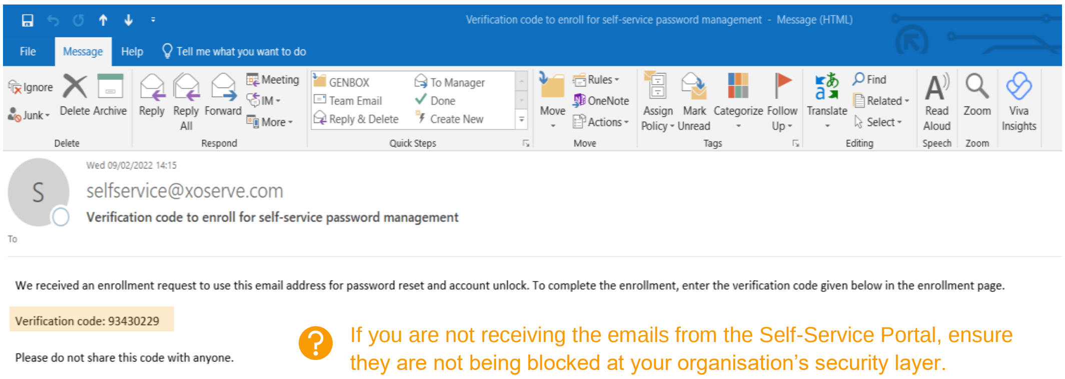
Enter the email address where you want to receive the verification code

user@organisation.com Send Code

Enter the code that you received via email

Enter verification code Verify Code

5) Check your inbox for the verification email from selfservice@xoserve.com and copy the Verification Code from the mail into your browser. Click the Verify Code button to complete the registration.



Wed 09/02/2022 14:15

selfservice@xoserve.com

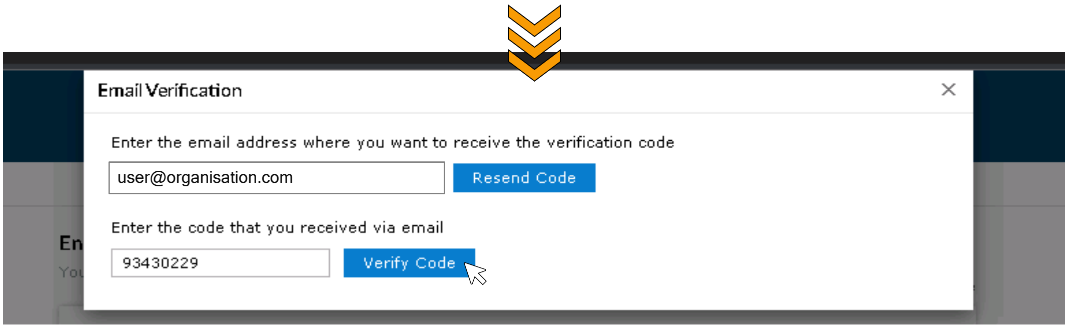
Verification code to enroll for self-service password management

We received an enrollment request to use this email address for password reset and account unlock. To complete the enrollment, enter the verification code given below in the enrollment page.

Verification code: 93430229

Please do not share this code with anyone.

If you are not receiving the emails from the Self-Service Portal, ensure they are not being blocked at your organisation's security layer.



Email Verification

Enter the email address where you want to receive the verification code

user@organisation.com

Enter the code that you received via email

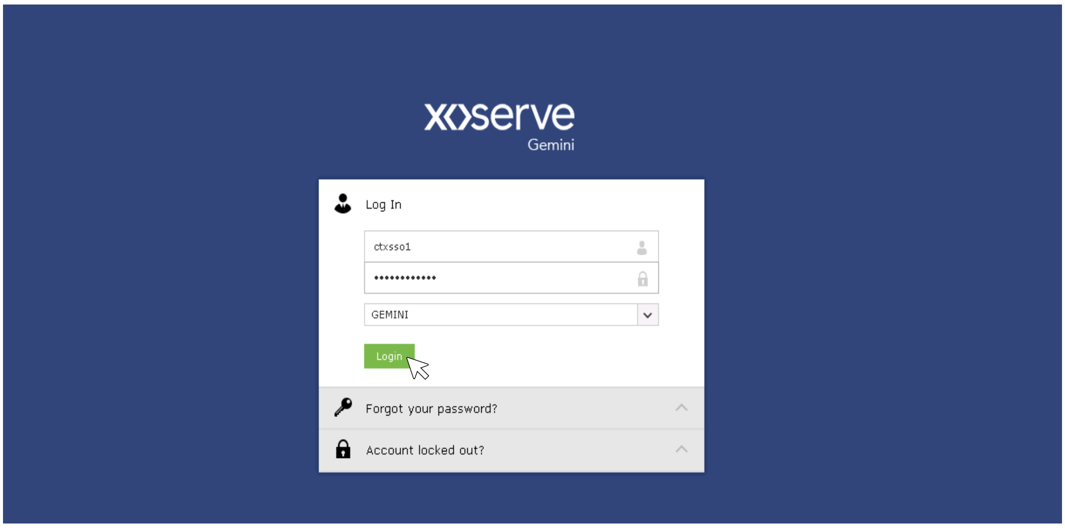
93430229

Self-Service: Password Reset (Step by Step)

1) Go to the Self-Service URL using your preferred desktop browser, with the link below. Alternatively, you can access via the Password Management hyperlink on the Gemini Citrix log-in page.

SSPR: https://selfservice.geminiwebservices.com/

2) Enter your Gemini Citrix username and password as normal and click the Log In button.



xoserve Gemini

Log In

ctxsso1

••••••••••••

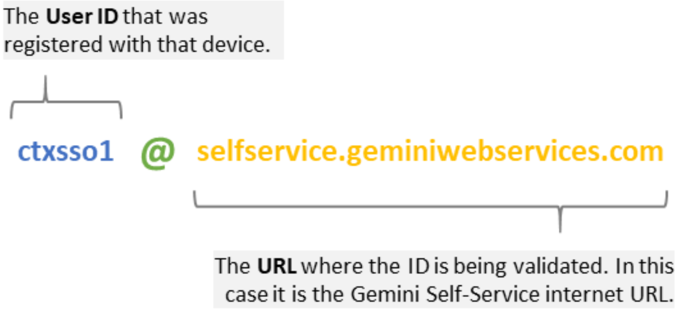
GEMINI

Login

Forgot your password?

Account locked out?

3) If you are using an authenticator application (Microsoft or Google), ensure you select the account that is linked to Gemini Self-Service. If you are having trouble identifying the correct code, it will usually be labelled using the syntax below.

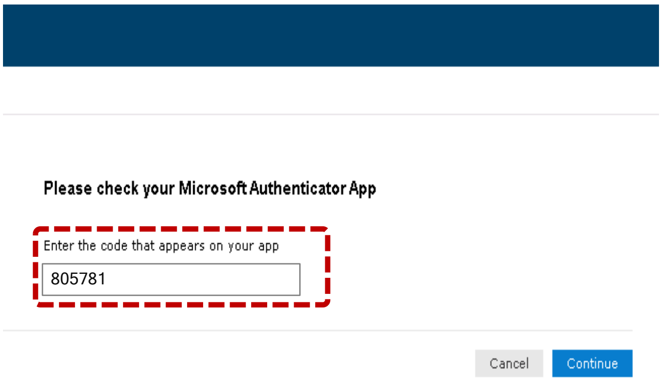


The **User ID** that was registered with that device.

ctxsso1 @ selfservice.geminiwebservices.com

The **URL** where the ID is being validated. In this case it is the Gemini Self-Service internet URL.

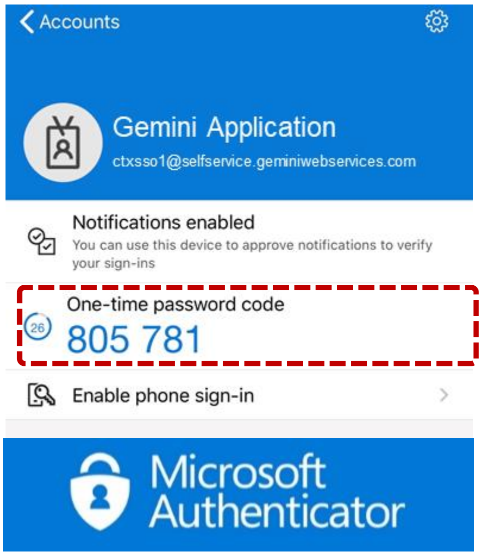
4) When prompted, enter the One-Time-Passcode via your chosen authentication method and click Continue to log-in to the Gemini Self-Service Portal. If you have not yet registered an authentication method, follow the previous section to complete the enrolment process.



Please check your Microsoft Authenticator App

Enter the code that appears on your app

805781



Gemini Application

ctxsso1@selfservice.geminiwebservices.com

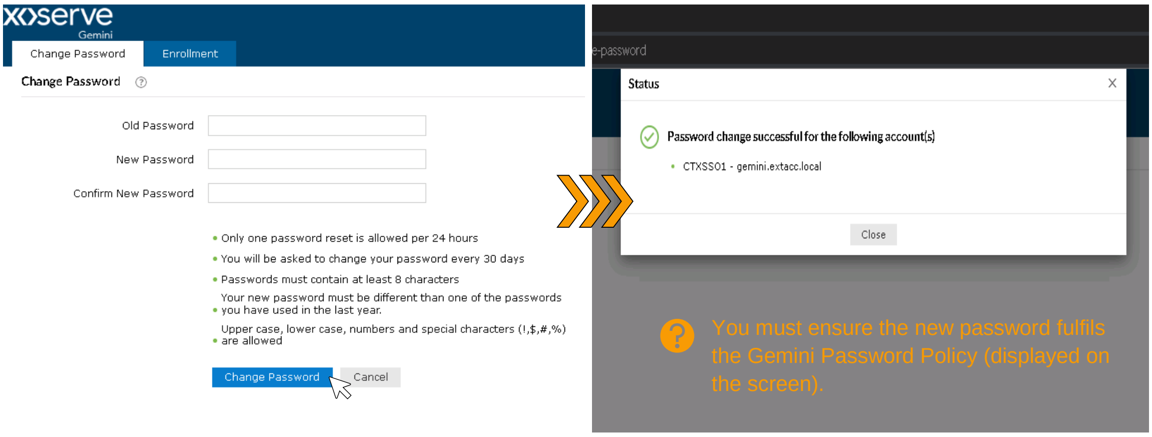
Notifications enabled

You can use this device to approve notifications to verify your sign-ins

One-time password code

805 781

5) From the Self-Service Portal, navigate to the Change Password tab and fill out the Old Password, New Password and Confirm New Password fields. Click on the Change Password button and you will receive a notification confirming the password has been changed.



Change Password

Old Password

New Password

Confirm New Password

- Only one password reset is allowed per 24 hours
- You will be asked to change your password every 30 days
- Passwords must contain at least 8 characters
- Your new password must be different than one of the passwords you have used in the last year.
- Upper case, lower case, numbers and special characters (!,$,#,%) are allowed

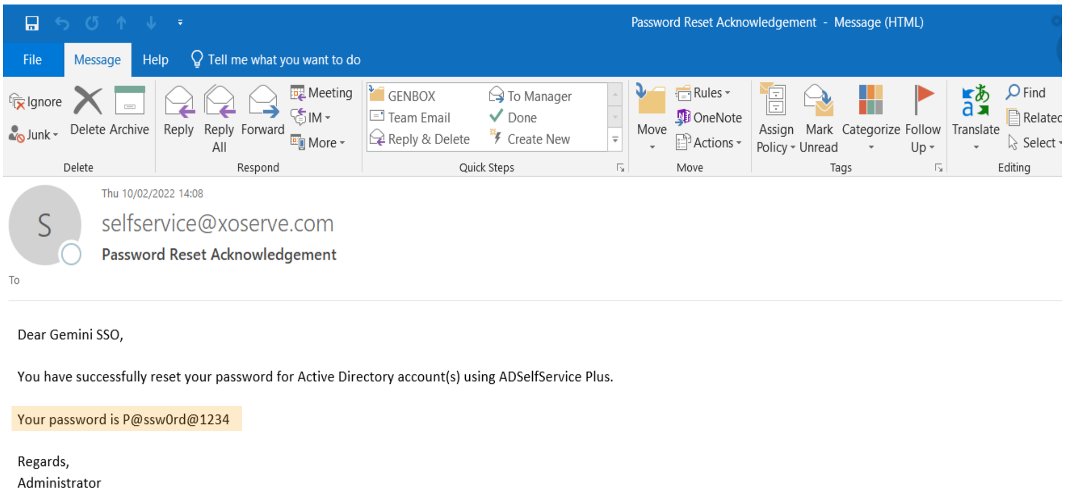
Status

Password change successful for the following account(s)

- CTXSSO1 - gemini.extacc.local

You must ensure the new password fulfils the Gemini Password Policy (displayed on the screen).

6) In addition to the browser notifications, you will also receive an email to your registered email addresses from selfservice@xoserve.com as confirmation of your new password.



Thu 10/02/2022 14:08

selfservice@xoserve.com

Password Reset Acknowledgement

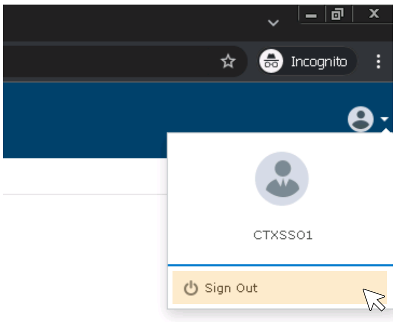
Dear Gemini SSO,

You have successfully reset your password for Active Directory account(s) using ADSelfService Plus.

Your password is P@ssw0rd@1234

Regards,
Administrator

7) To log out of the Self-Service Portal, click on the arrow in the top right of the page and select the Sign Out option.

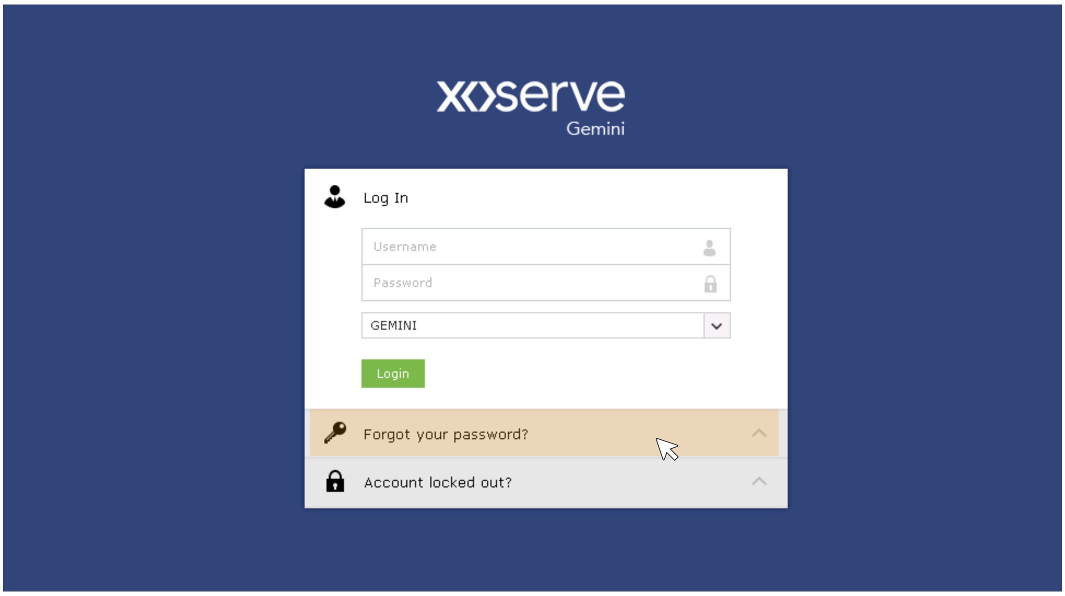


Self-Service: Forgotten Password (Step by Step)

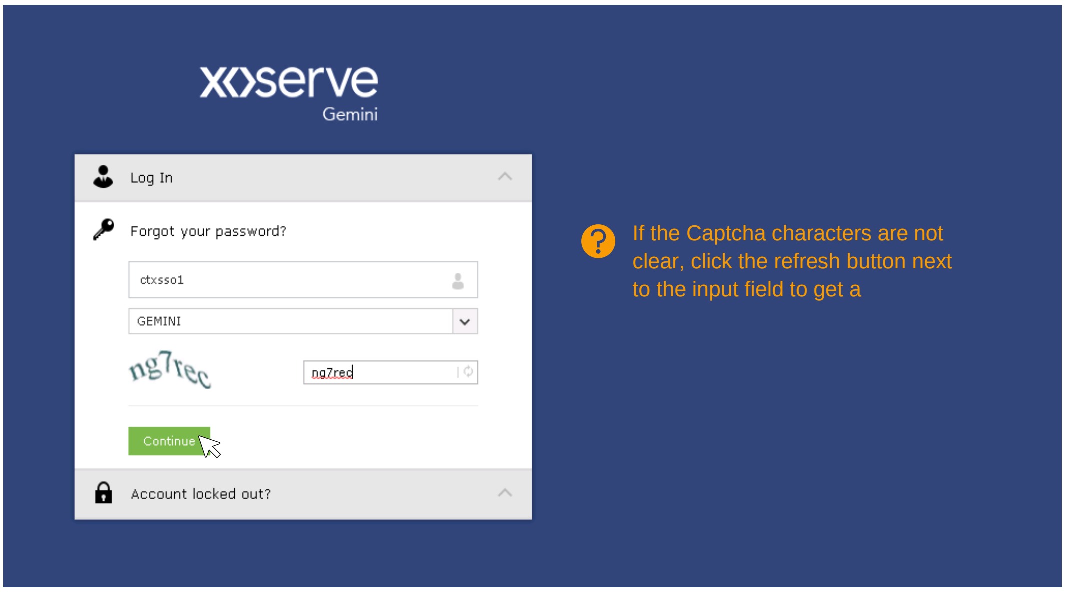
1) Go to the Self-Service URL using your preferred desktop browser, with the link below. Alternatively, you can access via the Password Management hyperlink on the Gemini Citrix log-in page.

SSPR: https://selfservice.geminiwebservices.com/

2) From the Self-Service log-in page, click on the Forgot Your Password option to reveal the additional fields.



3) Enter your Citrix username into the first field, then enter the string of text generated by the Captcha tool. Click Continue to move to the next stage.



ctxsso1

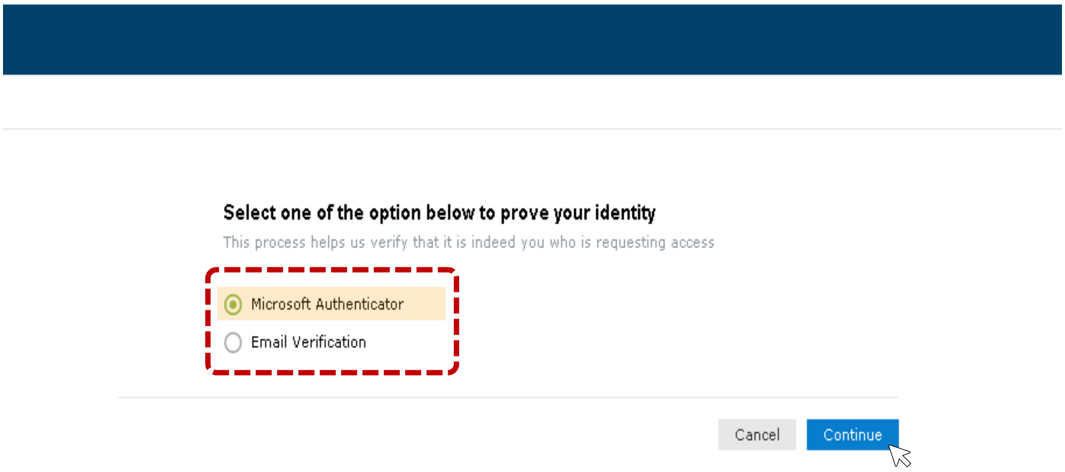
GEMINI

ng7rec

ng7red

If the Captcha characters are not clear, click the refresh button next to the input field to get a

4) Select your preferred authentication method from the options. If you have registered with a device using Google Authenticator, then this will appear on the list.



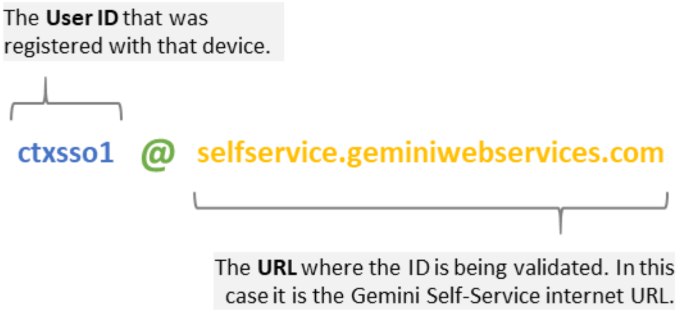
Select one of the option below to prove your identity

This process helps us verify that it is indeed you who is requesting access

● Microsoft Authenticator

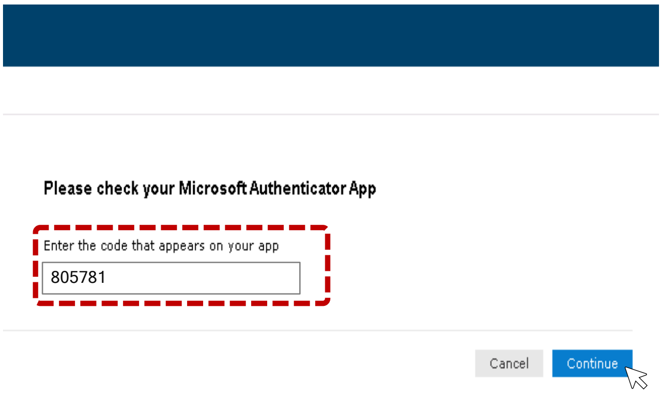
○ Email Verification

5) If you are using an authenticator application (Microsoft or Google), ensure you select the account that is linked to Gemini Self-Service. If you are having trouble identifying the correct code, it will usually be labelled using the syntax below.



The **User ID** that was registered with that device.
ctxsso1
@
selfservice.geminiwebservices.com
The **URL** where the ID is being validated. In this case it is the Gemini Self-Service internet URL.

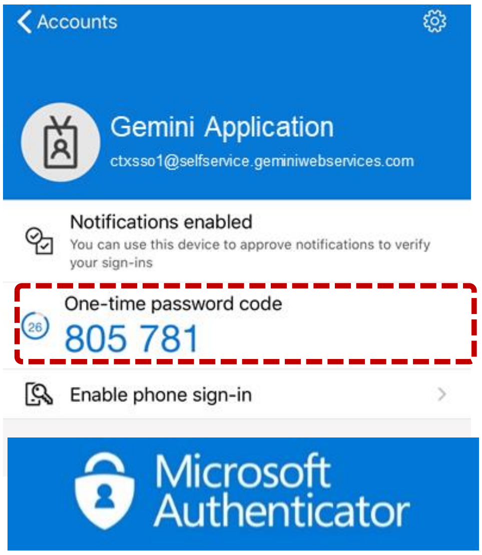
6) When prompted, enter the One-Time-Passcode via your chosen authentication method and click Continue to log-in to the Gemini Self-Service Portal. If you have not yet registered an authentication method, go back to the start of the SSPR section and follow the enrolment process.



Please check your Microsoft Authenticator App

Enter the code that appears on your app

805781



Gemini Application

ctxsso1@selfservice.geminiwebservices.com

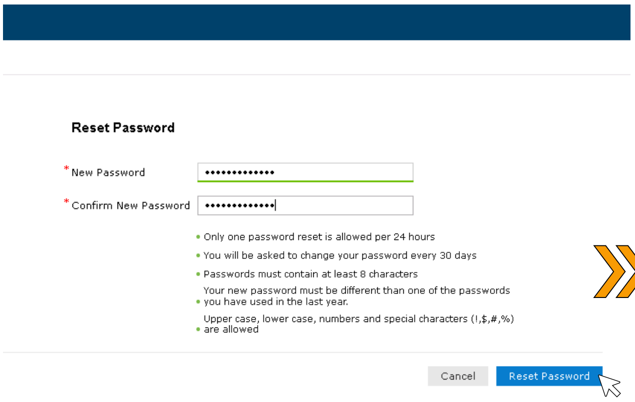
Notifications enabled

You can use this device to approve notifications to verify your sign-ins

One-time password code

805 781

7) Enter your new password twice in the fields provided, ensuring it adheres to the Gemini Password Policy given on the screen. Click the Reset Password button to complete the process and you will receive confirmation on the screen.

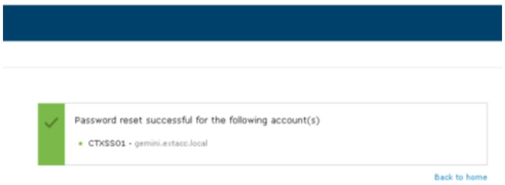


Reset Password

* New Password: •••••••••••••

* Confirm New Password: •••••••••••••

- Only one password reset is allowed per 24 hours
- You will be asked to change your password every 30 days
- Passwords must contain at least 8 characters
- Your new password must be different than one of the passwords you have used in the last year.
- Upper case, lower case, numbers and special characters (!,$,#,%) are allowed

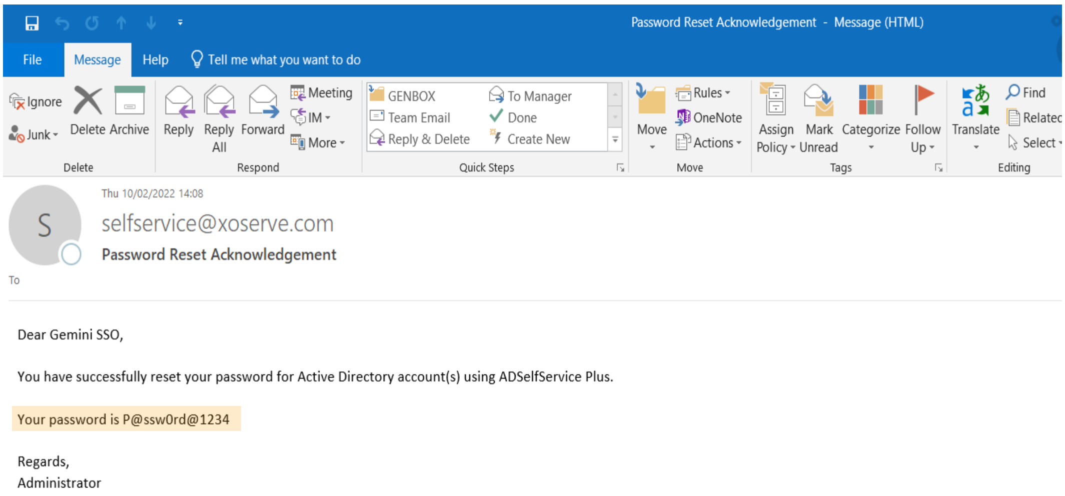


Password reset successful for the following account(s)

- CTXSSO1 - gemini.extacc.local

You must ensure the new password fulfils the Gemini Password Policy (displayed on the screen).

8) In addition to the browser notifications, you will also receive an email to your registered email addresses from selfservice@xoserve.com with confirmation of your new password.



Thu 10/02/2022 14:08

selfservice@xoserve.com

Password Reset Acknowledgement

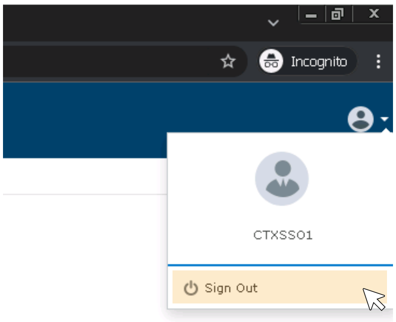
Dear Gemini SSO,

You have successfully reset your password for Active Directory account(s) using ADSelfService Plus.

Your password is P@ssw0rd@1234

Regards,
Administrator

9) To log out of the Self-Service Portal, click on the arrow in the top right of the page and select the Sign Out option.

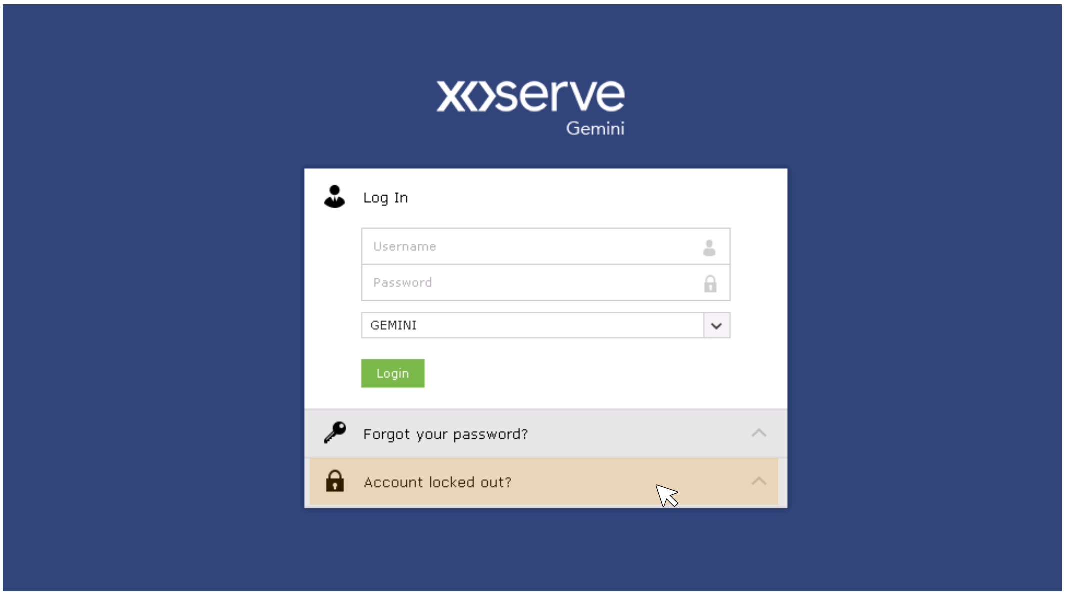


Self-Service: Account Locked (Step by Step)

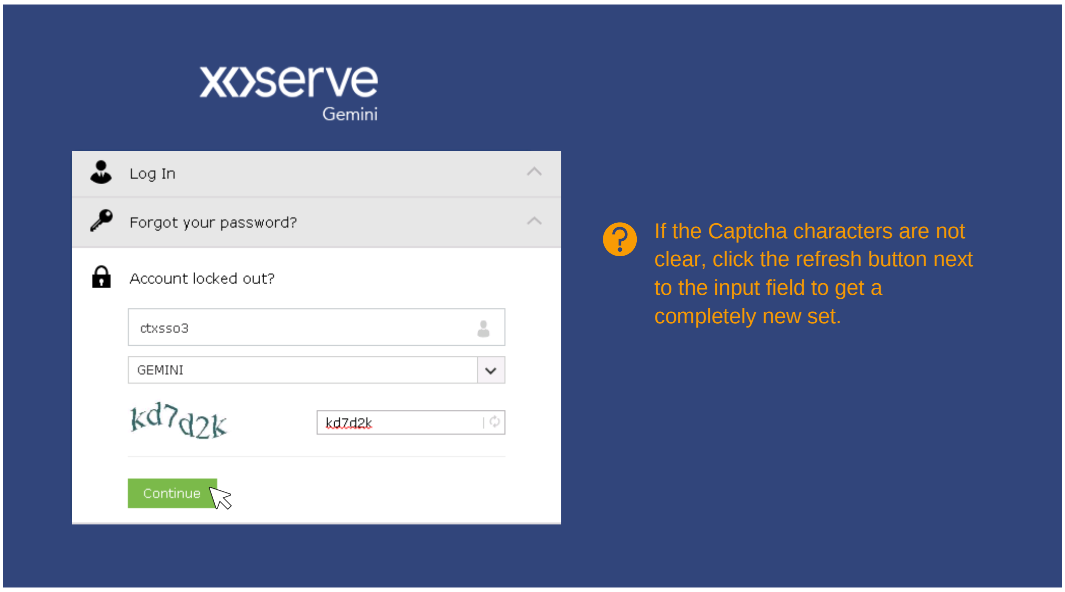
1) Go to the Self-Service URL using your preferred desktop browser, with the link below. Alternatively, you can access via the Password Management hyperlink on the Gemini Citrix log-in page.

SSPR: https://selfservice.geminiwebservices.com/

2) From the Self-Service log in page, click on the Account Locked option to reveal the additional fields.



3) Enter your Citrix username into the first field, then enter the string of text generated by the Captcha tool. Click Continue to move to the next stage.

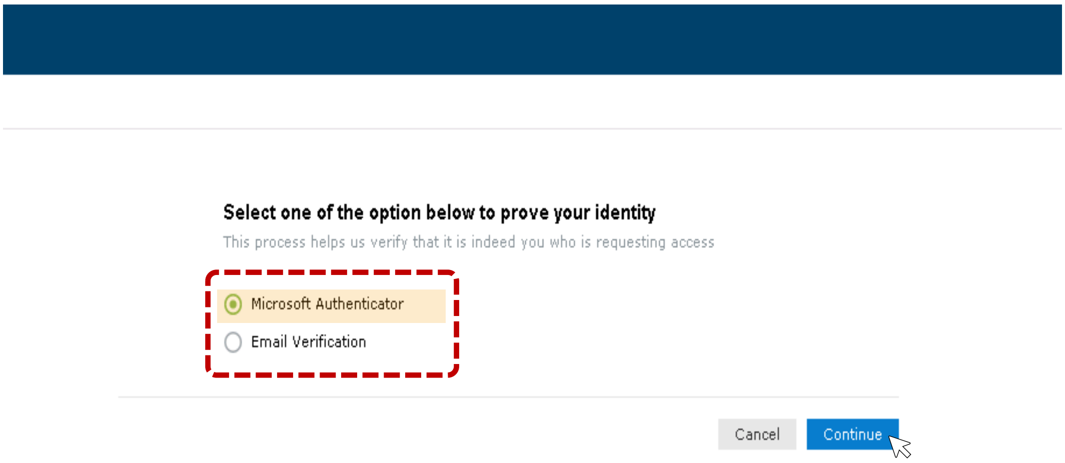


ctxsso3

kd7d2k

If the Captcha characters are not clear, click the refresh button next to the input field to get a completely new set.

4) Select your preferred authentication method from the options. If you have registered with a device using Google Authenticator, then this will appear on the list.



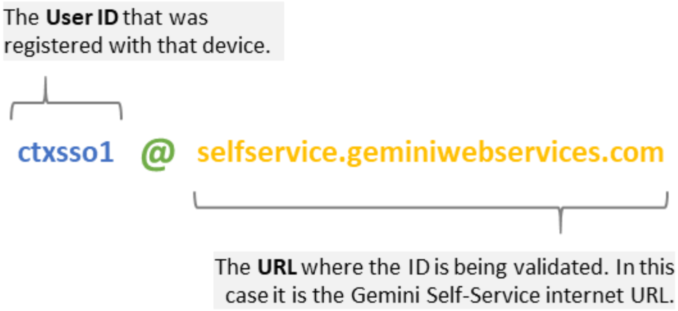
Select one of the option below to prove your identity

This process helps us verify that it is indeed you who is requesting access

● Microsoft Authenticator

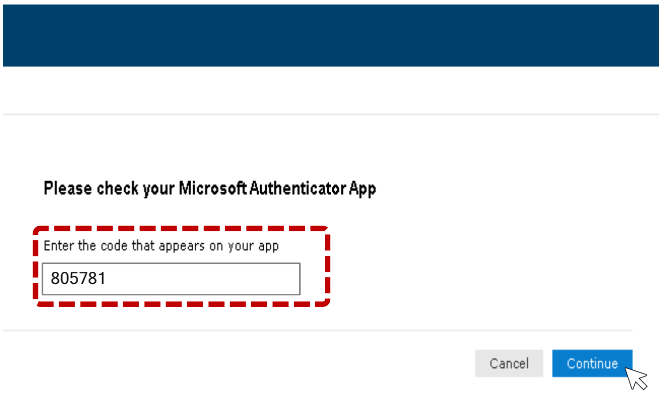
○ Email Verification

5) If you are using an authenticator application (Microsoft or Google), ensure you select the account that is linked to Gemini Self-Service. If you are having trouble identifying the correct code, it will usually be labelled using the syntax below.



The **User ID** that was registered with that device.
ctxsso1
@
selfservice.geminiwebservices.com
The **URL** where the ID is being validated. In this case it is the Gemini Self-Service internet URL.

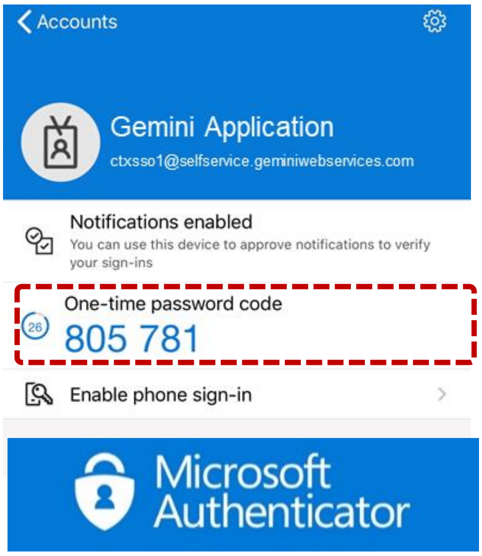
6) When prompted, enter the One-Time-Passcode via your chosen authentication method and click Continue to log-in to the Gemini Self-Service Portal. If you have not yet registered an authentication method, go back to the start of the SSPR section and follow the enrolment process.



Please check your Microsoft Authenticator App

Enter the code that appears on your app

805781



Gemini Application

ctxsso1@selfservice.geminiwebservices.com

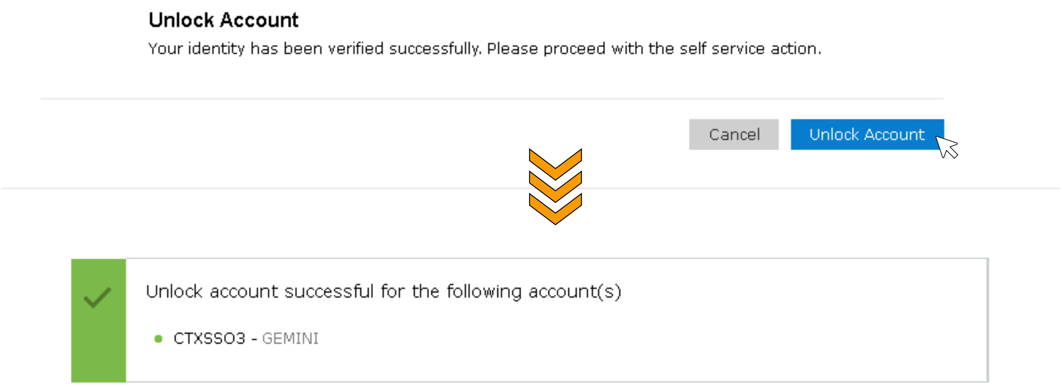
Notifications enabled

You can use this device to approve notifications to verify your sign-ins

One-time password code

805 781

7) Once your identity has been validated using the OTP, click on the Unlock Account button and you will receive confirmation on the screen that the account has been successfully unlocked.



Unlock Account

Your identity has been verified successfully. Please proceed with the self service action.

Unlock account successful for the following account(s)

- CTXSSO3 - GEMINI

Frequently Asked Questions (FAQs)

What happens if my Gemini Citrix and Gemini Application IDs do not match?

If your Gemini Citrix ID does not have a matching Gemini Application ID, you will be able to get past the first log-in screen and successfully access the Citrix homepage. However, when you click on the Gemini Production icon you will not be granted access to the Gemini Application and will likely be met with a HTTP 500 error page.

If you already know that your Gemini Citrix and Gemini Application IDs do not match, please contact the Service Desk immediately on **0845 600 0506** or via email to **servicedesk@xoserve.com**. Alternatively you can raise a ticket via our portal using this **link**.

What happens if my team share IDs to access Gemini?

If you use one Gemini Citrix ID but log-in to the Gemini application using a different ID, you will face issues post the introduction of the Single Sign-On functionality. If there is a Gemini Application ID that matches your Gemini Citrix ID then the SSO function will log you in to that matching ID. Practically, this may result in you having different roles to what you are used to and may even impact your ability to complete certain tasks. If your Gemini Citrix ID does not have a matching Gemini Application ID, then you will not be allowed access to the Gemini system.

Note: It is strongly advised that users **do not** share either Gemini Citrix or Gemini Application IDs – this is standard practice for maintaining good security in your organisation.

Do I need to perform any changes to access the new URLs?

If your organisation has tight restrictions on your internet traffic, it may be that the new URLs that have been published for the internet access and SSPR functionality are not accessible from your device. If this is the case, you will need to engage with your IT team to address the problem. To start, check that that URL is not blocked by your company firewall, proxy agent or VPN solution.

Can I use email as an authentication method to access Gemini over the internet?

Unfortunately, we do not offer this as an option at this stage. The current options for proving your identity are the Google or Microsoft authenticator mobile applications. These are completely free to download to your device and easy to set-up. If you are unsure on how to configure this, there is a detailed step by step guide in this document.

When do XP1 tokens expire?

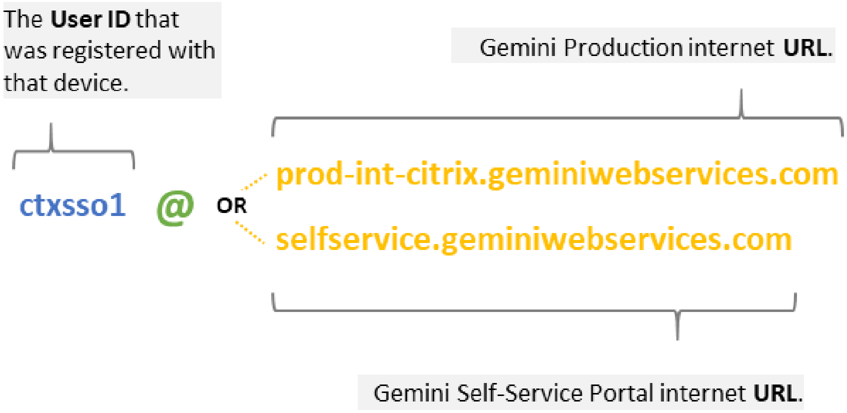
The current XP1 solution is due to be decommissioned at the end of June 2022. Post this date, if you want to access Gemini via contingency, you will need to go via the newly published internet-facing URL. Please be aware that you will need to set-up Multi-Factor Authentication for this route – a step by step guide is found in this document.

Internet Route: https://prod-int-citrix.geminiwebservices.com

Can I use the same Multi-Factor Authentication for the internet URL and the Gemini Self-Service Portal?

Since the Self-Service Portal is provided via a different route, it is not possible to use the same One-Time-Passcode (OTP) for both the SSPR and internet URL. However, it is possible to add multiple accounts to your Google or Microsoft authenticator application. When using the Multi-Factor Authentication, ensure you have entered the code which matches the service you are trying to use.

To distinguish between the codes, the authenticator application will usually follow the syntax below.


The User ID that was registered with that device.
Gemini Production internet URL.
ctxsso1
@
OR
prod-int-citrix.geminiwebservices.com
selfservice.geminiwebservices.com
Gemini Self-Service Portal internet URL.

Will these changes have any impact to my Gemini APIs?

Since the API connectivity comes down a different route, there is not expected to be any functional impact to the way APIs work or how they connect. However, whilst the change password command will not be impacted, the previous functionality to reset your API password via the Citrix page will no longer be available. The newly introduced Self-Service Portal will also not work with API accounts since it requires a matching Gemini Citrix ID to function, which APIs do not have.

It is still possible to request an API password reset via our Service Desk on **0845 600 0506** or via email to **servicedesk@xoserve.com**. Alternatively you can raise a ticket via our portal using this **link**.

What if I don’t want to use any new functionality?

If you are happy accessing Gemini via the current IX route, then the only change that will impact you is the Single Sign-On (SSO) functionality. Please go through the SSO section in this document to understand the pre-requisites and the detailed step by step guide.

Accessing Gemini over the internet and engaging with the Self-Service Portal for password management is completely optional. However, the XP1 tokens currently used for contingency are being decommissioned at the end of June 2022.