Electronic signature

Contents

Citrix RightSignature

July 6, 2022

Citrix delivers electronic signature ability using Citrix RightSignature. An electronic signature, sometimes known as an e-signature, is the same as your handwritten signature on a paper document, except electronic — a mark on an electronic contract or document you make to demonstrate your intent to agree to the terms of that document.

Integrating Citrix RightSignature with Citrix ShareFile gives you the power to obtain legally binding signatures on documents entirely online, being completed more quickly and securely than executing paper documents. Citrix delivers electronic signature capability at different levels:

- Citrix electronic signature integration with Citrix ShareFile lets you send files stored in your Citrix ShareFile account for electronic signature. For integration steps, see Getting started.
- Users can send for signature directly from Citrix Workspace with the integration described above (RightSignature to ShareFile), Citrix ShareFile enabled in Citrix Workspace, and electronic signature enabled for end users. For details of these setup processes, see Activate electronic signature licenses for Citrix Workspace users, Activate electronic signature licenses for ShareFile users (non-Workspace), and Add employee user.
- Citrix RightSignature is also available as a stand-alone solution. To get started, see Citrix RightSignature.

> **TIP:**
>
> Visit the Citrix User Help Center for electronic signature user information.

Fixed issues

June 26, 2022

This release addresses a number of issues that help to improve overall performance and stability.

January 20, 2021

This release addresses a number of issues that help to improve overall performance and stability.

RightSignature FAQs

For more information about RightSignature, see RightSignature FAQs.

Getting started

April 4, 2022

Electronic signatures are an easy and fast way to get documents signed online. These features give your organization the power to obtain legally binding signatures on documents entirely online — faster and more secure than paper documents.

Content Collaboration licenses are required to enable electronic signature features for your employee users. Once your Content Collaboration account is linked to a Citrix Cloud account, you can enable your users to send files stored in your Content Collaboration account for signature.

> **Note:**
>
> Visit the Citrix User Help Center for electronic signature user information.

Supported content

Electronic signatures are supported for documents that are fewer than 150 pages and less than 20 MB. Supported document types include:

- PDF
- Microsoft Word documents
- Plain text files
- Rich text files

> **Note**
>
> Format 3D PDFs to 8.5x11 and the same orientation on all pages.

Activate electronic signature licenses for Citrix Workspace users

Workspace administrators can log in to Citrix Cloud to verify electronic signature licenses are allocated and activated with in their linked Content Collaboration account.

> **Note**
>
> To use electronic signature features, Content Collaboration needs to be enabled and deployed for Workspace. For more information, see Deploy.

1. On the **Citrix Cloud dashboard**, select **Manage Content Collaboration**.
2. Under the **Manage** tab, select the **Admin Overview**.

Under **Allocated licenses**, view a number of employee licenses available for Electronic Signature features. See Add users to enable employee users with Send for Signature and other Electronic signature permissions.

Activate electronic signature licenses for Content Collaboration users (non-Workspace)

Content Collaboration administrators can log in to the web application to verify electronic signature licenses are allocated and activated with in their Content Collaboration account.

1. Select **Settings**.
2. Select **Admin Settings**.
3. Select **Admin Overview**.

Under **Allocated licenses**, view a number of employee licenses available for Electronic Signature features. See Add employee users with e-signature access in Configure to enable employee users with e-signature sending capabilities and other permissions.

Activate electronic signature licenses for ShareFile users

ShareFile administrators can log in to the web application to verify electronic signature licenses are allocated and activated with in their ShareFile account.

1. Select **Settings**.
2. Select **Admin Settings**.
3. Select **Admin Overview**.

Under **Allocated licenses**, view a number of employee licenses available for Electronic Signature features. See Add employee users with e-signature access in Configure to enable employee users with e-signature sending capabilities and other permissions.

> **Note**
>
> Electronic signatures licenses allow 100 documents per employee license to be sent per month. For example, an account with 10 employee licenses can send 1,000 documents in a month. These licenses are pooled together for the entire account. An individual employee user can send 100 or more documents in a month given there are enough licenses available in the pool.

Firewall considerations

Allow web traffic

To connect users from your on-premises environment to communicate with the Citrix RightSignature Control Plane for Electronic signature features, authorize HTTPS/TLS 1.2 traffic to the following IPv4 addresses and *.rightsignature.com domain:

Control Plane IP addresses

CIDR Notation	IP Address	Netmask
199.255.192.0/22	199.255.192.0	255.255.252.0

CIDR Notation	IP Address	Netmask
199.127.232.0/22	199.127.232.0	255.255.252.0
54.240.0.0/18	54.240.0.0	255.255.252.0

Allow email notifications

Enable incoming email notifications for users on your on-premises environment. Configure email security gateways and spam filters for trusted hosts using the IPv4 and email addresses to receive Electronic signature-related email notifications:

Notification IP address
208.117.51.168

Notification email addresses
documents@rightsignature.com
support@rightsignature.com

For other Content Collaboration related Firewall Configurations, see CTX208318.

Integrations

See Enable integrations for more information on available integrations to configure for Citrix RightSignature electronic signature capabilities.

Two-step verification

Citrix strongly recommends the use of two-step verification as an extra layer of security to reduce the likelihood of any unauthorized access to Citrix accounts. Two-step verification uses your phone to provide an extra layer of security for your user name. After you sign in, you are asked to enter a verification code that is sent to your phone using a text message (SMS) or voice call. Some apps require an app-specific password that must be generated each time you want to sign in to the app.

> **Note**
>
> Two-step verification does not apply to accounts that sign in with Citrix Workspace. Two-step ver-

> ification is automatically enabled for Citrix Cloud accounts. It is managed by the account owner.

Configure electronic signatures

October 4, 2021

RightSignature allows you to customize your account including branding, integrations, and more.

Requesting API keys

Log into your RightSignature account to request an API key and manage your API credentials. For more information on requesting API keys, see RightSignature Resources.

Send and prepare documents

Electronic signature allows you to send documents to one or more parties. You can prepare a document for someone to sign in person. No emails or authentication needed.

Send document for signature

There are several ways to begin sending a document for electronic signature. Some workflows can begin in the Content Collaboration account or directly start a document in the Citrix RightSignature app.

After selecting a document to send for signature, employee users will be automatically redirect to the Citrix RightSignature browser app to prepare the document for sending.

Start Documents for signature in Citrix RightSignature and select from the following options:

- Bulk send for signature

> **Note:**
>
> To send each signer their own copy of the document, select an existing template.

- Send for signature
- Sign a document yourself
- Create a reusable template
- Send a document package

Prepare a document for signature

After selecting a sending method, select a supported file type (PDF, TXT, DOC, DOCX or RTF) from an available storage source.

Select **Prepare Document** to continue. The document will automatically convert into a PDF file to serve as the background for preparing a form or document ready for signature.

For more information on sending a document for signature, see the Citrix User Help Center article Send for signature.

Templates

Utilizing templates allow employee users to skip the document creation process with reusable documents ready to send for signature. Users with electronic signature sending capabilities can create template documents when logged into the Citrix RightSignature App.

Manage template settings

For employee users, select **User Access**. Under **E-signature settings**, select **Manage e-signature templates**. Users with the base level permission can create, edit, and delete their own templates and send template documents created by others. With Manage e-signature templates permissions, users can edit, delete, and send template documents created by others.

Create a template

Users can choose a new document to upload or select an existing document from storage. The template editor allows the user to prepare a document by adding signer and sender roles, document overlays, and merge field options.

A templates creator or employee users with the permissions to manage e-signature templates can edit or delete templates on the Citrix RightSignature app.

For more information on creating an electronic signature template, see the Citrix User Help Center article Create a template.

Edit a template

Follow these steps to edit an existing template:

1. Select **Templates** in the left menu bar, then select the template that you want to edit from the menu.
2. Select **Details**, and on the Details screen select **Edit**.

3. If replacing the underlying source file used to create the template, select the red x. Afterwards, select the new source file of the template.
4. Select **Prepare Document** to continue editing. You will first be able to edit the roles on the template - change the role names, edit the order, or add/delete roles. When finished with editing the roles, click **Next: Place Fields**.
5. Next use the document overlay options to add, change, and remove various types of fields. When finished with edits to the document, click Next: Review.
6. Edit the name, message, tags, expiration, and carbon copies for this template.
7. When you are finished editing, select **Create Template**.

For more information on editing an electronic signature template, see the Citrix User Help Center article Edit a template.

Verify account settings

Use the account section in RightSignature to configure the settings for administrative tasks. Use **Settings** to verify changes to your account including:

- Your Information - this includes your name, email, and avatar.
- Account Information - this includes your company name, account name, and your current plan.
- Verified Emails - You can add email addresses to send for signature. The dashboard displays all documents sent to any of these verified email addresses.

Require passcode for documents

Once enabled, a passcode is necessary to sign the document.

Default token expiration period

This feature lets you set an expiration for the request signature links sent.

Blue ink signatures

Select blue ink signature to distinguish a signed original from a photocopy. All original copies will display the signature in blue.

Enable integrations

Allow all your users to view and set the connection with other apps you use. By toggling it off, none of the users will be able to view the Integrations settings to enable/ disable the out-of-box integrations. This is to help centrally control all your users' access to the available integrations.

Use the following information to integrate RightSignature into other applications.

To enable Google contact integrations, see RightSignature - Google Contacts Integration.

To enable Google Drive integrations, see RightSignature - Google Drive Integration.

To enable Podio integrations, see RightSignature - Podio Integration.

To enable Stripe integrations, see RightSignature - Stripe Integration.

Customize branding for signing experience

Branding options include setting up your company logo, color background and email header options.

1. Select **Account**.
2. Select **Branding**.

For more information on branding, see Set up your company branding in RightSignature.

Reports

The following reports are available in RightSignature:

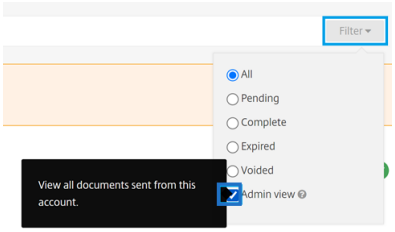
- **Overview report** - displays the total number of documents sent. This report also provides the average number of documents sent, viewed, and signed. Users are ranked in this report on the number of documents sent each month.
- **Efficiency report** - compares the number of signed documents and the total number of documents sent each month. This ratio, presented as a percentage, reflects how efficiently each user collects signatures when sending documents.
- **Cycle time report** - displays the average amount of time required to view and sign each users document. These figures reflect how quickly recipients are to execute each users document on a monthly basis.
- **Data exporter** - exports the signing data from every copy of a Reusable Template, or every document with a shared tag. The data can be exported as a CSV file. The Data Exporter only pulls data from documents completed from the latest version of a template. Editing a template creates a new version so the Data Exporter will not return data from documents completed before the template was edited.
- **Enterprise report** - provides account administrators on Enterprise level accounts the ability to export a complete list of all of the documents sent during a particular month. The data can be exported as a CSV file.
- **New usage report** - provides account administrators on Enterprise level accounts the ability to export the number of sent and signed documents, as well as the median cycle time, for each user.

Add employee user

To add an employee user with electronic signature access, create or edit an employee user in the People section of your Content Collaboration account. Under User Access then E-signature settings, select Send documents for e-signature. The base level permission is suitable for standard users. One e-signature license is required to grant the permissions to electronic signature sending capabilities for supported files. Users can sign in and access templates and additional settings for the files they send for signature directly from the Citrix RightSignature app.

View all electronic signature documents

From User Access and E-signature settings, select View all e-signature documents. Users with the base level permission can also view all e-signature documents if logged into the Citrix RightSignature App. Use the base level permission when creating or editing an employee permitted to view all legal and secure documentation sent by other users with electronic sending capabilities.
Login into the Citrix RightSignature app, to view all the documents sent from this account. On the Documents tab, in the Search Documents bar, click Filter, select All and check the Admin view box.



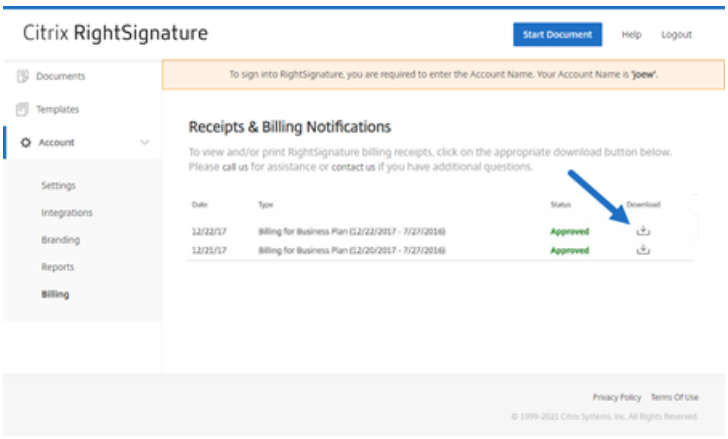
Billing and invoices

Receipts & Billing Notifications

To view or print billing receipts for your account, click the appropriate date on this page. You can request an email notification when your account is billed.

View receipts and billing notifications

The **Receipts & Billing Notifications** link in the **Admin Settings > Admin Overview > Billing** section allows any user with this permission enabled to download copies of any receipt or invoice for the account.



Security

April 4, 2022

This article applies to electronic signatures using RightSignature. Utilizing up to 256-bit EV SSL encryption by DigiCert and the world-class server infrastructure of Amazon Web Services (AWS), our electronic signature capability ensures the privacy of our users' data. RightSignature incorporates the most advanced security solutions, giving you the same level of data protection and redundancy as an online bank.

Backups

RightSignature user data is stored in Amazon S3 data centers. Every document and piece of data is automatically and immediately copied to multiple locations for redundancy. Therefore, there is no lag time in backup creation, ensuring data would be available instantly after an interruption in any one location.

Physical security

Critical AWS facilities boast substantial setbacks and military-level perimeter control barriers. Professional security teams control physical access at the perimeter and building entrances with intrusion detection systems, video monitoring, and other electronic techniques. Only after passing two-factor authentication tests may authorized staff access data center floors.

Online security

Once logged in, your connection with RightSignature is secure and encrypted using industry-leading SSL technology. RightSignature's data storage on Amazon S3 is accessible only via SSL encrypted

endpoints, ensuring your electronic signature data cannot be viewed or compromised in transit from your internet node to the AWS secured facility. In addition, a firewall with default deny mode and definitive traffic restrictions protects your data in storage.

Legal

September 22, 2021

The U.S., Canada, the UK, Australia, New Zealand, and many countries around the world have enacted laws providing electronic contracts the same legal validity and enforceability of pen-and-paper contracts. Electronic signature is the trusted and secure solution for obtaining electronic signatures that fulfill key requirements of the Electronic Signatures in Global and National Commerce (E-SIGN) Act and the National Conference of Commissioners on Uniform State Laws' Uniform Electronic Transactions Act (UETA). The world's largest companies rely on electronic signature, and users have executed millions of contracts using electronic signature.

"There is a significant movement toward signing legal documents electronically. You can sign legally binding contracts online and even from your phone. With electronic signature you can upload contracts and have them signed in a faster, cheaper, and more secure way than paper documents." - GP Solo

E-signature laws

Citrix electronic signature capability utilizing RightSignature is designed to address the key requirements of:

The Electronic Signatures in Global and National Commerce (E-SIGN) Act, Pub. L. No. 106-229, 114 Stat. 464 (2000) (15 U.S.C. §§7001-7031);
The Uniform Electronic Transactions Act (UETA), as approved by the National Conference of Commissioners on Uniform State Laws in 1999 (7A Pt. 1 U.LA. 211, 211-99 (2002)); and many state laws modeled after UETA.

These e-signature laws are intended to encourage the rapid adoption of digital signatures and decrease the use of antiquated paper methods. Under E-SIGN, a contract "may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation." 15 U.S.C.A. § 7001(a)(2). Similarly, under Section 7(d) of UETA, if a law requires a signature, an electronic signature satisfies the law. Furthermore, E-SIGN provides that any state's law is preempted if and to the extent that it does not comply with UETA or its substantial equivalent. 15 U.S.C.A. § 7002. While these e-signature laws reinforce the validity of many types of electronic agreements, the laws do not cover certain types of documents, such as statutes, regulations, or other rules of laws governing wills, codicils, testamentary trusts, adoption, divorce, or other matters of family

law, certain commercial transactions, certain court documents, and certain notices, generally do not affect substantive requirements of otherwise applicable substantive law, and contain requirements for creating enforceable agreements.

Intent to sign

One of the primary criteria for a valid e-signature is whether the e-signature evidences a clear intent by the signatory to sign. Electronic signature's capture of a real handwritten signature provides evidence of the signer's intent to execute the document. Furthermore, electronic signature's second-generation handwritten signature capture technology addresses potential legal issues that may arise with first-generation click-to-sign systems, because handwritten signatures cannot be inadvertently affixed to contracts and uniquely identify a signer whereas click-to-sign buttons can easily be inadvertently clicked and clicked by others who have access to a signer's computer or smartphone.

Signature associated with document

Under E-SIGN and UETA, a compliant electronic signature must be an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. 15 U.S.C.A. § 7006(5); UETA §2(8). Electronic signature locks down the executed document with the signature record and produces a Signature Certificate that includes the handwritten signature graphic and an auditable activity log. In addition, when you use our drag-and-drop signature boxes, electronic signature places the handwritten signature at the appropriate locations inside the document.

Consumer disclosures

E-SIGN allows electronic documents and records with electronic signatures to comply with statutes, regulations, or other rules of law that require that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing if the consumer has provided affirmative consent to such use and has not withdrawn the consent, and the consumer, prior to consenting, receives a clear and conspicuous statement of certain information and provides certain consents. 15 U.S.C.A. § 7001(c). Electronic signature users may address the E-SIGN disclosure and consent requirements by enabling a Consumer Disclosure Page for each document and requiring other parties to consent to certain terms prior to executing contracts. Electronic signature also allows potential signatories the ability to opt out from receiving or executing electronic contracts.

Tamper-proof record

After signing, electronic signature secures your executed document with a complex hash algorithm to ensure the permanent record is tamper-proof.

Document access and storage

Section 7001(d) of E-SIGN and Section 12(a), (b), (d) and (e) of UETA contain requirements for record-keeping. Contracts executed with electronic signatures are delivered in Portable Document Format to signatories so that they can retain them for the periods prescribed by any applicable statutes of limitations. Electronic signature stores your documents in a secure archive for the duration of the time you maintain a paid account, utilizing the world-class data infrastructure of Amazon Web Services for security and redundancy.

Audit log

Section 13 of UETA states that evidence of a record or signature may not be excluded from being admissible evidence solely because it is in electronic form. Every document sent through electronic signature includes a detailed audit log, complete with time stamps, identity authentication, and other critical information. Electronic signature can provide a legal foundation to introduce the documents as evidence and have courts enforce them.

Authentication

Electronic signature employs a proprietary, multivariate identity authentication system. Components include email address validation, biometric signature analysis, IP address capture, and the collection of other identifiers unique to each signing party.

Technology neutrality

Electronic signature is platform-agnostic. Parties e-sign on any computer, using any web browser, with no downloads and no plug-ins. This technological neutrality gives all recipients an equal opportunity to execute documents without impediment.

Disclaimer

This overview of particular e-signature laws is not a comprehensive overview of the requirements of e-signature laws in the United States or other countries, is for educational and informational purposes only, and is not intended, and should not be construed, as legal advice.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States