

DigiCert UltraDNS Failover



Keep critical applications available, even when infrastructure fails.

Intelligent monitoring and automated DNS failover

For organizations that depend on always-on digital services, even a brief outage can impact revenue, productivity, customer trust, and business continuity. As applications become increasingly distributed across cloud, hybrid, and on-premises environments, maintaining availability requires more than infrastructure redundancy. It requires intelligent, automated failover.

DigiCert® UltraDNS Failover continuously monitors the health of your critical applications and automatically redirects traffic when an outage is detected. Built directly into the UltraDNS platform, Failover delivers enterprise-grade monitoring and DNS failover without requiring additional hardware, software, or complex deployments.

Built on DigiCert UltraDNS

Failover is powered by the globally distributed DigiCert UltraDNS network, providing reliable health monitoring and automated failover for internet-facing applications.

Monitoring agents located around the world continuously perform protocol- and transaction-based health checks against your configured endpoints. Each endpoint is monitored from multiple geographic locations to ensure accurate failure detection and minimize false positives.

When predefined health thresholds are exceeded, Failover automatically updates DNS responses to direct users to healthy standby resources. Once the primary service has recovered, traffic is automatically restored. Administrators receive real-time notifications throughout the process, providing complete visibility into service status.

Key capabilities



Continuous global health monitoring

Monitor applications from multiple global locations using protocol- or transaction-based health checks to quickly detect service degradation or outages.



Automated DNS failover

Automatically redirect users to healthy infrastructure when failures occur, and restore traffic once services recover.



Flexible traffic control

Support simple primary/secondary failover and more advanced traffic management configurations by integrating Failover with UltraDNS traffic management capabilities.



Administrative control

Override automated decisions when needed, schedule planned failovers for maintenance windows, or configure monitoring-only deployments.



Real-time notifications

Receive email alerts whenever monitored services change status, enabling faster operational response.

Monitoring capabilities

Failover supports monitoring for a wide range of internet-facing services, including:

- ICMP (Ping)
- HTTP and HTTPS
- TCP
- SMTP
- FTP
- Transaction and content validation
- Custom ports and proprietary services

Monitoring is performed from multiple globally distributed locations to improve detection accuracy and reduce false positives.

Additional deployment options

Failover supports a variety of operational scenarios, including:



Manual failover during emergency situations



Scheduled failover for planned maintenance



Configurable delay before failover or restoration



Monitoring-only mode with alerting



Transaction-based monitoring of applications and back-end services

Customer benefits



Increase application availability with automated failover



Reduce downtime through continuous health monitoring



Simplify disaster recovery without additional infrastructure



Deploy quickly with a fully managed cloud service



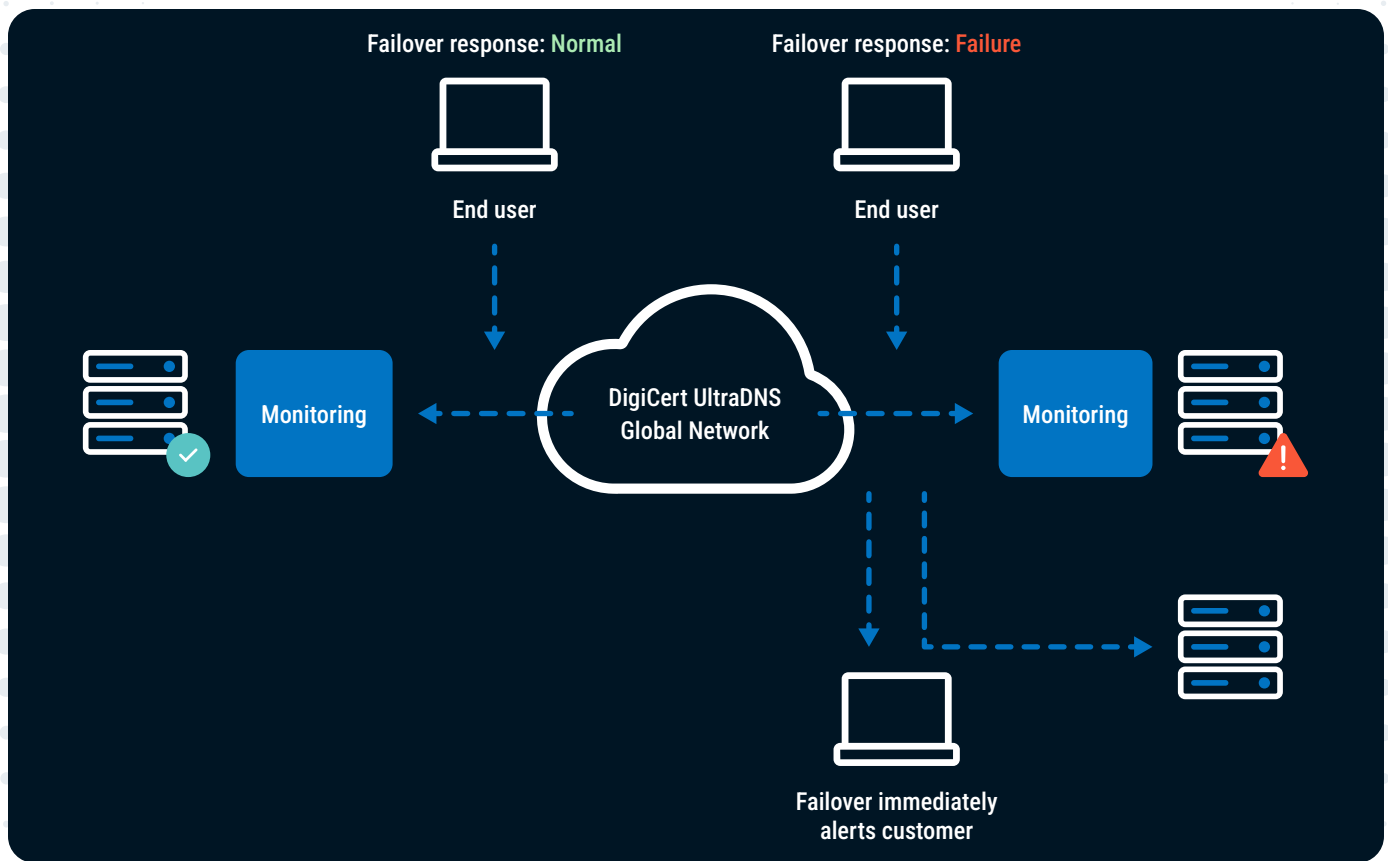
Scale effortlessly across global environments



Improve operational efficiency through automation

Features

- Enterprise-grade monitoring and automated DNS failover
- Integrated directly into DigiCert UltraDNS
- Global health monitoring network
- DNSSEC-enabled DNS infrastructure
- Web-based management portal and REST API
- Real-time email notifications
- 24×7×365 DigiCert global support



How Failover works

1. Failover continuously monitors your primary and standby infrastructure from multiple global monitoring locations.
2. When a service fails configured health checks, Failover verifies the outage across multiple monitoring points.
3. DNS responses are automatically updated to direct users to healthy standby resources.
4. Once the primary service has recovered, Failover automatically restores traffic to the preferred endpoint.
5. Administrators receive notifications throughout the process, providing complete visibility into service health and failover events.

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.

© 2026 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.